VLAN and Its Implementation over ATM By Using IP: A Communication

Kunal Deswal[1] , Shweta Thakur[2]
1 (Student, Dept. of Information Technology DCE, Gurgaon, India)

ABSTRACT

In computer networking, a single layer-2 system may be divided to make different unique broadcast domains, which are commonly detached with the goal that packets can just pass between them through one or more routers; such an area is alluded to as a Virtual Local Area Network, Virtual LAN or VLAN. This is normally accomplished 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 advanced gadgets can check packets through tagging, with the goal that a single interconnect (trunk) may be utilized to transport information for different Vlans. Grouping hosts with a typical set of prerequisites paying little heed to their physical location by VLAN can extraordinarily simplify network design. A VLAN has the same qualities as a physical local area network (LAN), however it considers end stations to be assembled together all the more effectively regardless of the fact that they are not on the same network switch. VLAN membership can be designed through software rather than physically relocating devices or connections. Most undertaking level networks today utilize the idea of virtual Lans. Without Vlans, a switch considers all interfaces on the switch to be in the same broadcast domain.

Key words-
VLAN; Router; Switch; Domain

1. INTRODUCTION

To understand Vlans, it is first important to have an understanding of Lans. A Local Area Network (LAN) can for the most part be characterized as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can speak with one another without the requirement for a router. Communications with devices on other LAN segments obliges the utilization of a router. Virtual Lans (Vlans) can be seen as a gathering of devices on diverse physical LAN segments which can impart with one another as though they were along the same physical LAN segment. Switches utilizing Vlans make the same division of the network into particular broadcast domains however don't have the latency problems of a router. Switches are additionally a more cost effective solution.

2. USES OF VLAN

Network draftsmen set up Vlans to give the segmentation services generally gave just by routers in LAN configurations. Vlans address issues such accessability, security, and network administration. Routers in VLAN topologies give broadcast filtering, security, address rundown, and traffic-flow administration. By definition, switches may not bridge IP traffic between Vlans as doing so would disregard the integrity of the VLAN broadcast domain. Vlans can likewise help make 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 give the adaptability to adjust to changes in network necessities and take into account improved administration. Apportioning a local network into a few unique segments for e.g.

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

in a typical infrastructure imparted crosswise over VLAN trunks can give an abnormal state of security with incredible adaptability to a nearly ease. Quality of Service plans can upgrade traffic on trunk links for realtime (Voip) or low latency prerequisites (SAN). Vlans could likewise be utilized within a school or work environment to give simpler access to local networks, to take into consideration simple administration, and to anticipate disturbance on the network.In cloud computing Vlans, IP addresses, and MAC addresses on them are assets which end users can oversee. Setting cloud-based virtual machines on Vlans may be desirable over straight forwardly on the Internet to dodge security issues.

3. VLAN TYPES

There are 2 Types of VLAN

- Three basic VLAN memberships for determining and controlling how a packet entering a switch gets assigned to a VLAN.
- The network IP subnet address can be used to classify VLAN membership
- IP addresses are used only as a mapping to determine membership in VLAN's.
- In Layer 3 VLAN’s; users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses.

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. Each device associated with one of its ports can send packets to any of the others. Dividing ports by VLAN groups divides their traffic truly like uniting the devices to an alternate, unique switch of their own. Configuration of the first custom VLAN port group normally includes uprooting ports from the default VLAN, such that the first custom group of VLAN ports is really the second VLAN on the device, not withstanding 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 just pass through an intermediate switch by means of two pass-through ports, just the two ports must be a part of the VLAN, what's more are tagged to pass both the obliged VLAN and the default VLAN on the intermediate switch. Administration of the switch obliges that the administrative capacities be connected 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 consistently group networks with the goal that the network location of clients is no more so firmly coupled to their physical location.

4.1 TECHNOLOGIES ABLE TO IMPLEMENT VLAN 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 communications standard. *Why ATM?* ATM natively supports a specific Quality of Service. ATM is defined and available at higher speeds 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 Service Providers (ISPs) to make use of an ATM core, to interconnect a number of IP routers. Looking back to the early 1990s, Internet Service Provider (ISP) networks consisted of routers interconnected by leased lines. Examples of leased lines are E1 and E3 in 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 empowers the utilization of low cost equipment which gives rapid speed forwarding.

- Additionally traffic engineering is exceptionally hard to just as load the resources on a network is possible by doling out metrics to distinctive links In practice this is very simpler to perform traffic engineering by manually characterizing Pvcs.

5.1 ISSUES OF RUNNING IP OVER ATM

- IP is connectionless addressing
- IP routing
- ATM is connection orientated
- ATM addressing
- ATM routing
- ATM signaling

As per the focuses we have made as such, we can see that internetworking IP and ATM is not new, yet is made and demonstrated combo. Actually, ATM is as of now the empowering technology for the Internet.

5.2 PROBLEMS FACED IN INTER-NETWORKING

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.
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:
  47.00918100000006170530118.00400
  BFF001
  3.00 (Written in hexadecimal)
- IP Address 4 Bytes: 220.190.40.56 (Written in dotted decimal notation)

IP locations and ATM locations are totally diverse. There is no connection between them, that is, an ATM location does not contain an IP address. On the off chance that you are given simply an ATM location of a specific segment, you can't derive that part's IP address straightforwardly from the ATM address. Review that ATM locations is 20-bytes long, comprising of a 13- byte prefix, a six byte end station identifier and an one-byte selector field. The prefix is allocated by a director, yet the end station identifier part is the MAC location of the ATM interface. Accordingly, ATM addresses are sure to particular interfaces. By differentiation, an IP location is 4 bytes long and is doled out by a director. IP addresses just have a logical binding to interfaces.

6. VLAN OPERATION

So as to encourage routing between IP subnet VLAN, each one switch needs to know the location of the router. Each switch must have no less than one port that is on the forwarding way to the router. This can be accomplished by having the router sending periodic multicast VLAN packet to all the switch ports that are in hybrid or trunk mode. Switch port that gets this packet must be part of all Vlans, generally the routing methodology won't work. Consistently, the active router conveys 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 neighbouring 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 quantity of packets need to be sent into the network to keep up this IP subnet VLAN are equivalent to the quantity of active spanning tree links in the network in addition to the link to the router.

7. PROS & CONS OF VLAN

7.1 PROS

1. 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.
2. 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.
3. Flexibility - at the allocation from nodes to network segments, independent from the physical location.
4. 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.

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 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 - Utilizing a network switched with Vlans is less expensive than making a routed network with lavish routers as routers cost a great deal all the more then switches by and large.

7.2 CONS

VLAN’s Limit - it is conceivable to make just 4094 separate Vlans for the same network, in light of the 12 bit VID identifier. Every VLAN has it interesting ID somewhere around 0 and 4096, whereby 0 and 4096 are reserved, along these lines the switch knows where to route the frame. This ought to be all that could possibly be needed throughout today, in many organizations yet could demonstrate as a bottleneck later on in the same way Ipv4 did. Managerial Overhead - when utilizing hard configured Vlans, for example, port based or MAC based it requires a considerable amount of managerial work to deal with the networks as they advance and change with time. Then again the use of Subnet based VLANS requires stronger switches which cost more cash, furthermore includes extra switching latency in light of the fact that it is obliged to decode the layer 3 header somewhat.

12. REFERENCES

[1]. Chan WaiKok, M. Salim Beg Simple IP Subnet VLAN Implementation 1Faculty of Information Technology, 2 Faculty of Engineering Multimedia University, CyberJaya, 63100, Malaysia, Ninth IEEE International Conference on 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.

[4]. Ahmavaara, K., Haverinen, H., & Pichna, R. (2003). Interworking architecture between 3GPP and WLAN systems. *Communications Magazine, IEEE*, *41*(11), 74-81.

[5]. Feng, W. C., Kaiser, E., & Luu, A. (2005, March). Design and implementation of network puzzles. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE* (Vol. 4, pp. 2372-2382). IEEE.