Design to Improve S*3 for a Multilayer-Switched Network in an Institution

Meenakshi Sundaram.K[1], Karthik.B[2], Harihara Gopalan.S[3]

1. Lecturer ,Sri Ramakrishna Engineering College ,
Coimbatore . India .
meenaksji@gmail.com

2. PG Scholar, IGNOU,
New Delhi. India .
karthikbellan@yahoo.com

3. PG Scholar, PSG College of Arts&Science,
Coimbatore. India .
urshari@gmail.com

Abstract. The design and implementation of structured computer and communication network are based on the requirement of an individual, feasibility and application services planned on the network. Modification in the network infrastructure if any must minimize the changes in the network infrastructure with minimum down time. Layered network design attracts most of the organization due to its adoptability, security and scalability. In the layered approach, the fault identification is simple. By implementing Virtual LAN (VLAN) one can suppress the broadcasting, implement access list for security and slice the bandwidth based on application. Security measures can also be considered into the design without much modification by implementing the local security policy. We propose a layered network design for an academic institution to cover entire campus with high-speed data, QoS on multimedia information as well for video lectures with scalability and security aspects.

Keywords: Switched Network , *Scalability ,* Securability ,*Service

1 Introduction

Information networks have emerged as strategic [6] assets and a critical element for delivering education and services. Today's information networks must meet increasing demands to carry more information and provide new services. Leading educational institutions are adopting newer applications for education and information dissemination. The educational institutions participate in research and development activities in addition to the conventional teaching to keep ties with the industry and this leads driving forces for the improvement of network infrastructure and

© A. Gelbukh, S. Torres, I. López (Eds.)
Advances in Computer Science and Engineering
Research in Computing Science 19, 2006, pp. 147-156

technology decisions. In educational institutions, the computers are connected with Local Area Network (LAN) technology and (WAN) Wide Area Network for their various Internet applications and Wireless LAN and WAN [11] for research activities. To be success in R&D activities students are required to refer the electronic form of recent literature, journal of referred. Network access from student hostels and academic departments will promote self-education and learning. The purpose of this paper is to describe the proposed multilayer-switched [2] infrastructure for networking the entire campus [1] to improve network service and security [4]. For smooth running of Institute Network some local security policies and practices must be implemented. The paper also describes security considerations while rapid access to various forms of information to the student community. The proposed design includes application considerations as well as technical considerations while designing a converged infrastructure. The network security and system security are two important issues, should be addressed by any academic institution. The Scope of this paper addresses the infrastructure that will be enabled on the IP multi services infrastructure for various forms of network service including wireless WAN adoptability and security to access campus resources and access to Internet.

2 Multilayer-Switched Network Design Architecture

Multilayer-switched network design architecture includes three layers [5] such as

- The backbone (core) layer that provides optimal transport between sites
- The distribution layer that provides policy-based connectivity [8]
- The local-access layer that provides workgroup/user access to the network

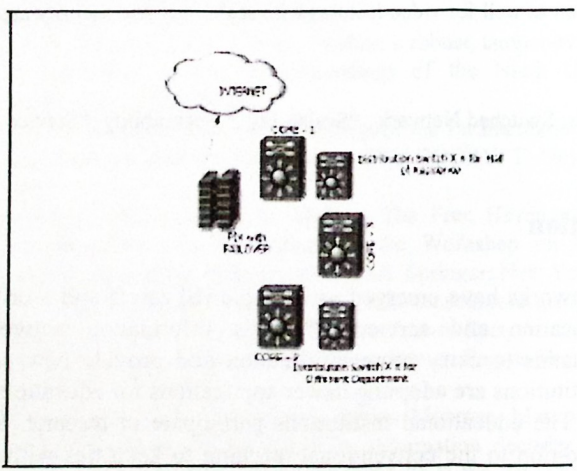

Fig 1. A typical multi-layer Switched Backbone

Each student hostel and the Major academic departments will have a high speed layer 3 aggregation switches with local servers. Edge switches, which connect to the student, faculty or lab workstations will aggregate the end connections to the

distribution switch. The core switches will provide high-speed transport and switching for the entire campus network infrastructure.

Figure 1, we show the Layer 3 switched campus backbone with dual links to the backbone from each distribution-layer switch. The main advantage of this design is that each distribution-layer switch maintains two equal-cost paths to every destination network, so recovery from any link failure is fast. This design also provides double the trunking capacity into the backbone Layer 3 switched backbones have several advantages such as Reduced router peering, Flexible topology with no spanning-tree loops, Multicast and broadcast control in the backbone and Scalability to arbitrarily large size.

3 Various Layers Of The Multi-Layer Switched Backbone

3.1 Local-Access Layer

It will provides high speed 10 Mbps / 100 Mbps Ethernet connection to the end station / desktop computer on Category 5/6 UTP (copper) cabling. The maximum number of user connections required at the each floor of a wing and is depends on the port density of the switch. It can be easily replaceable in case of failures and is manageable from central location with network management station and supports converged services on IP such as telephony and video. Layer 2 managed switches capable of segregating users based on VLANs (Broadcast domains). The access layer is the point at which local end users are allowed into the network. This layer may also use access lists [10] or filters to further optimize the needs of a particular set of users to enforce the local security policy. In the campus environment, access-layer functions can includes such as shared bandwidth, switched bandwidth, MAC layer filtering and micro segmentation.

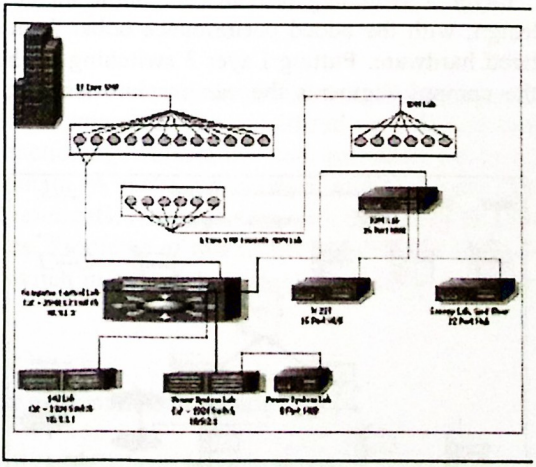

Fig 2. Network Schematic of the Local-Access Layer

3.2 Distribution Layer

It provides high-speed 100 Mbps Ethernet connections / gigabit Ethernet connection [3] to the Department/Hostels on Category 5/6 UTP (copper) cabling. It aggregates all the gigabit Ethernet uplinks on single mode fiber from the access switches at the different areas of the hostels. It is modular and scalable both in terms of expansion and performance. The distribution layer of the network is the demarcation point between the access and core layers and helps to define and differentiate the core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place. In the campus environment, the distribution layer can include several functions, such as address or area aggregation, departmental or workgroup access, broadcast/multicast domain definition, Virtual LAN (VLAN) routing, any media transitions that need to occur and security. It is manageable from central location with network management station. It supports converged services on IP such as telephony and video, security and access control lists to protect common resources such as network infrastructure switches and critical servers from pilferage and attacks. It can connect to the core switches at the central core switch.

3.3 Backbone (core) Layer

It provides high-speed gigabit switching between the distribution switches. It should be completely redundant. The inter-link between the core switches and the distribution switch will use the single mode fiber infrastructure. It should be manageable from the network management station. It supports converged services on IP such as telephony and video. The core layer is a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer of the network should not perform any packet manipulation; such as access lists and filtering that would slow down the switching of packets. The Campus network is used multilayer-switched Network. Layer 3 switching provides the same advantages as routing in campus network design, with the added performance boost from packet forwarding handled by specialized hardware. Putting Layer 3 switching in the distribution layer and backbone of the campus segments the campus into smaller, more manageable pieces.

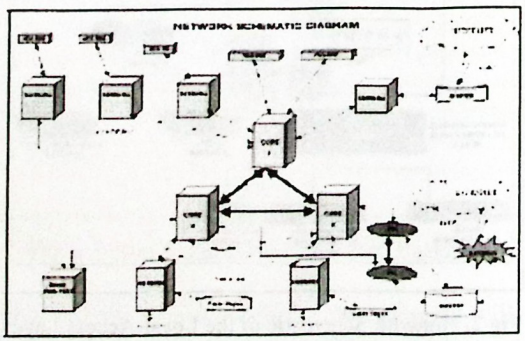

Fig 3. Complete network schematic of the layered network

4 Principles Of The Design Of Layered Network

Good-layered network design [5] is based on many concepts that are summarized by the following key principles:

Examine single points of failure carefully—There should be redundancy in the network so that a single failure does not isolate any portion of the network. There are two aspects of redundancy that need to be considered are backup and load balancing. In the event of a failure in the network, there should be an alternative or backup path. Load balancing occurs when two or more paths to a destination exist and can be utilized depending on the network load. The level of redundancy required in a particular network varies from network to network.

Characterize application and protocol traffic: - The flow of application data will profile client-server interaction and is crucial for efficient resource allocation, such as the number of clients using a particular server or the number of client workstations on a segment.

Analyze bandwidth availability: - There should not be an order of magnitude difference between the different layers of the hierarchical model. It is important to remember that the hierarchical model refers to conceptual layers that provide functionality. The actual demarcation between layers does not have to be a physical link—it can be the backplane of a particular device.

Build networks using a hierarchical or modular model: - The hierarchy allows autonomous segments to be inter-networked together.

5 Multilayer-Switched Infrastructure To Improve Network Service And Security: Implementation Issues

5.1 Reducing the size of Failure Domain

A group of Layer 2 switches connected together is called a Layer 2 switched domain. The Layer 2 switched domain can be considered as a failure domain because mis configured or malfunctioning workstation can introduce errors that will impact or disable the entire domain. A jabbering network interface card (NIC) may flood the entire domain with broadcasts. A workstation with the wrong IP address can become a black hole for packets. Problems of this nature are difficult to localize. Restricting it to a single Layer 2 switch in one wiring closet if possible should reduce the scope of the failure domain.

5.2 Limiting the Size of Broadcast Domain

Media Access Control (MAC)-layer broadcasts flood throughout the Layer 2 switched domain. Use Layer 3 switching in a structured design to reduce the scope of broadcast domains. In order to do this, the deployment of VLANs and VLAN trunking is

needed. Ideally one VLAN (IP subnet) is restricted to one wiring-closet switch. The gigabit uplinks from each wiring-closet switch connect directly to routed interfaces on Layer 3 switches.

5.3 Avoidance of Spanning-Tree for Redundancy

Layer 2 switches run spanning-tree protocol to break loops in the Layer 2 topology. If loops are included in the Layer 2 design, then redundant links are put in blocking mode and do not forward traffic. It is preferred to avoid Layer 2 loops by design and have the Layer 3 protocols handle load balancing and redundancy, so that all links are used for traffic. The spanning-tree domain should be kept as simple as possible and loops should be avoided. With loops in the Layer 2 topology, spanning-tree protocol takes between 30 and 50 seconds to converge. Use Layer 3 switching in a structured design to reduce the scope of spanning-tree domains. Let a Layer 3 routing protocol, such as Enhanced Internet Gateway Routing Protocol (IGRP) or Open Shortest Path First (OSPF); handle load balancing, redundancy, and recovery in the backbone.

6 VLAN Design And Configuration

6.1. Perfect VLAN Design

VLAN has the same characteristics of a failure domain, broadcast domain, and spanning-tree domain, as described above. So, although VLANs can be used to segment the campus network logically, deploying pervasive VLANs throughout the campus adds to the complexity. Avoiding loops and restricting one VLAN to a single Layer 2 switch in one wiring closet will minimize the complexity. With the advent of high-performance Layer 3 switching in hardware, the VLANs can be used to logically associate a workgroup with a common access policy as defined by access control lists (ACLs). Similarly, VLANs can be used within a server farm to associate a group of servers with a common access policy as defined by ACLs.

6.2 Configuration of VLAN

When you configure VLANs, the network can take advantage of the following benefits and they are

Broadcast control—Just as switches physically isolate collision domains for attached hosts and only forward traffic out a particular port, VLANs provide logical collision domains that confine broadcast and multicast traffic to the bridging domain.

Security—If you do not include a router in a VLAN, no users outside of that VLAN can communicate with the users in the VLAN and vice versa. This extreme level of security can be highly desirable for certain projects and applications.

Performance—You can assign users that require high-performance networking to their own VLANs. You might, for example, assign an engineer who is testing a

multicast application and the servers the engineer uses to a single VLAN. The engineer experiences improved network performance by being on a "dedicated LAN," and the rest of the engineering group experiences improved network performance because the traffic generated by the network-intensive application is isolated to another VLAN.

Network management—Software on the switch allows you to assign users to VLANs and, later, reassign them to another VLAN. Recabling to change connectivity is no longer necessary in the switched LAN environment because network management tools allow you to reconfigure the LAN logically in seconds.

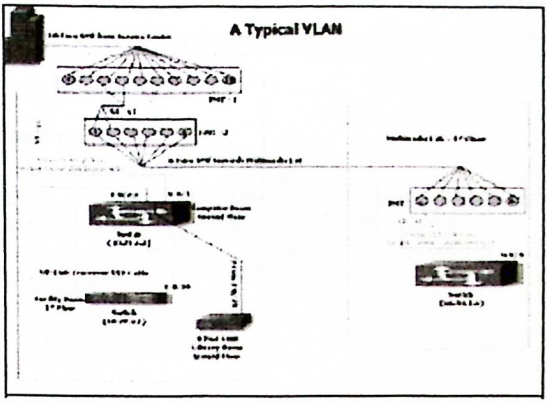

Fig 4. Schematic of a typical VLAN

6.3 IP Subnet Planning for the Campus

An IP subnet also maps to the Layer 2 switched domain; therefore, the IP subnet is the logical Layer 3 equivalent of the VLAN at Layer 2. The IP subnet address is defined at the Layer 3 switch where the Layer 2 switch domain terminates. The advantage of subnetting is that Layer 3 switches exchange summarized reachability information, rather than learning the path to every host in the whole network. Summarization is the key to the scalability benefits of routing protocols, such as Enhanced IGRP and OSPF. In an ideal, highly structured design, one IP subnet maps to a single VLAN, which maps to a single switch in a wiring closet. This design model is somewhat restrictive, but pays huge dividends in simplicity and ease of troubleshooting.

6.4 Policy Domain

Access policy is usually defined on the routers or Layer 3 switches in the campus network. A convenient way to define policy is with ACLs that apply to an IP subnet. Thus, a group of servers with similar access policies can be conveniently grouped together in the same IP subnet and the same VLAN. Other services, such as DHCP are defined on an IP subnet basis.

7 Quality Of Service For Voice And Video And Caching

7.1 Quality of Service for Voice and Video

Interface experiences congestion when it is presented with more traffic than it can handle. Network congestion points are strong candidates for Quality of Service (QoS) mechanisms. A better alternative is to apply congestion management and congestion avoidance at oversubscribed points in the network. Figure 5 shows the examples of typical congestion points

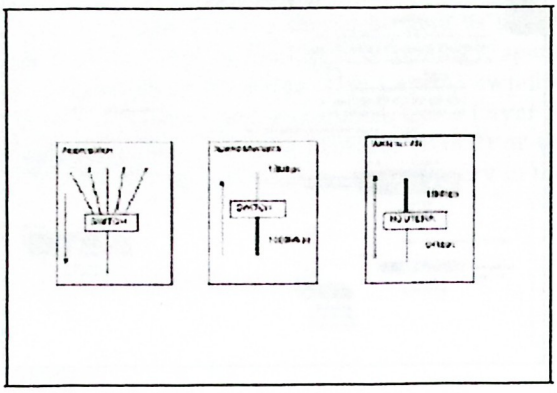

Fig 5. Typical congestion points

Network congestion results in delay. A network and its devices introduce several kinds of delays, as explained in Understanding Delay in Packet Voice Networks. Variation in delay is known as jitter, as explained in Understanding Jitter in Packet Voice Networks. Both delay and jitter need to be controlled and minimized to support real-time and interactive traffic. In particular, QoS features provide better and more predictable network service by different methods such as Supporting dedicated bandwidth, Improving loss characteristics, Avoiding . and managing network congestion, Shaping network traffic and Setting traffic priorities across the network.

7.2 Scaling with Caching

As enterprises grow and expand their network over Internet or to remote locations on WAN, it becomes very critical to improve the response to the enterprise web servers and to reduce delay across WAN. Typical Web caching solutions involve a series of caching devices in close proximity to a specific user community. Content Caching works best if cache engines are positioned closest to the points of access to minimize WAN bandwidth utilization. An enterprise can deliver accelerated service to its customers by front-ending Web server farms with cache engine clusters. In this application, content requests are redirected to a cache engine cluster instead of directly forwarding them to the Web servers. If the content being requested is

cacheable, the cache engines will fill the request. When the cache cluster fulfills these requests, it off-loads traffic from the Web servers, thereby minimizing content download latency and increasing Web server capacity. Therefore, once a customer requests a particular piece of cacheable content, it is cached so that successive requests are not directed repeatedly to a Web server. The same concept can be extended to the enterprise LAN as well. Intranet servers with rich multimedia content are often the potential bottlenecks. The content can be moved closest to the user community with high-speed cache engines.

8 IP Address Scheme And Network Address Translation

8.1 Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internet [9]
10.0.0.0
10.255.255.255 (10/8 prefix)
172.16.0.0
172.31.255.255 (172.16/12 prefix)
192.168.0.0
192.168.255.255 (192.168/16 prefix)

An institute that decides to use IP addresses out of the address space defined in this document can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the institute, or the set of institute, which choose to cooperate over this space so they may communicate with each other in their own private Internet. Private hosts can communicate with all other hosts inside the institute, both public and private. However, they cannot have IP connectivity to any host outside of the institute. While not having external (outside of the institute) IP connectivity private hosts can still have access to external services via mediating gateways (e.g., application layer gateways). Two scalability challenges facing the Internet are the depletion of registered IP address space and scaling in routing. Network Address Translation (NAT) [7] is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As its name implies, NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network.

9 Conclusion

We have designed a layered switched network for an academic institution. This design takes provides high-speed data down to the end point. The fault identification is found

to be easy. The security policies can be implemented at the VLAN's. VLAN suppresses the broadcasting into the local domain and so we avoid bandwidth choking. The downtime of the core and distribution level is taken care by the redundancy. This design provides effective use of effective IP address space by using private IP addresses and network address translation.

References

1. CISCO AVVID Campus Solution .
   http://www.itworld.com/WhitePapers/Cisco_AVVID_Campus/
2. CISCO Inter-network Design Guide
   http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm
3. Fiber Optics
   http://www.fols.org/pubs/whitepaper0100.html
4. Firewall
   http://www.firewallsdirect.com/white_papers/watchguard/fb_wp_ltr.pdf
5. Gigabit Campus Network Design— Principles and Architecture .
   http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.htm
6. IT Strategic Plan for an academic institute .
   http://athena.uwindsor.ca/units/its/itsp/ITSPWFinal.nsf/
5. University+Website?OpenForm
7. Network address Translation .
   http://www.cisco.com/warp/public/732/nat/
8. Network Connectivity Solutions .
   http://www.intel.com/network/connectivity/solutions/
9. Private IP address .
   http://www.isi.edu/in-notes/rfc1918.txt
10. What do you need for network security?.
    http://business.cisco.com/prod/tree.taf%3Fasset_id=87144&
    public_view=true&kbns=1.html
11. Wireless Wan network .
    http://www.intel.com/network/connectivity/resources/doc_library/documents/
    pdf/np1692-01.pdf