2002

Analyzing the costs/tradeoffs involved between layer 2, layer 3, layer 4 and layer 5 switching

Gautam Kapur

Analyzing the Costs/Tradeoffs Involved Between Layer 2, Layer 3, Layer 4 and Layer 5 Switching

By

Gautam Kapur

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
Of
Computing and Information Sciences

February 22, 2002

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College Of Computing and Information Sciences

Analyzing the Costs/Tradeoffs Involved Between Layer 2, Layer 3, Layer 4 and Layer 5 Switching

I, Gautam Kapur, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 4/31/02 Signature of Author: _____

Rochester Institute of Technology

B. Thomas Golisano College
Of
Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: Gautam Kapur

Thesis Title: Analyzing the Costs/Tradeoffs Involved Between Layer 2, Layer 3, Layer 4 and Layer 5 Switching

Thesis Committee

Name	Signature	Date
Professor Luther Troell Chair		4/22/02
Professor Jim Leone Committee Member		4/22/02
Professor Charlie Border Committee Member		4/22/02

Table of Contents

1	Methodology & Abstract.	1
2	Layer 2 Switching.	2
3	Switching Basics.	5
3a	Switch Forwarding Techniques.	7
3b	Switch Path Control.	11
4	Layer 2 Switching Process.	18
5	Types of Switching.	22
5a	Cut Through Switching.	22
5b	Store and Forward Switching.	23
6	Types of Buffering.	24
6a	Input Port Buffering.	24
6b	Output Port Buffering.	25
7	Functions of Layer 2 Switching.	25
8	Benefits of Layer 2 Switching.	26
9	Layer 3 Switching.	27
10	Performance Parameters in Layer 3 Switching.	30
10a	Packet Switching.	30
10b	Route Processing and Management.	31
10c	Intelligent Network Services.	34
11	Tradeoff's in using Layer 3 Switches.	40
11a	Layer 2 Switches Vs Routers.	40
11b	Layer 3 Switching & Bandwidth utilization.	44
11c	Layer 3 Switch Philosophy.	46
12	Benefits of Layer 3 Switching.	47
13	Standard based Layer 3 Switching Architectures.	47
13a	Multi Protocol over ATM.	48
13b	Multi Protocol Label Switching.	49
14	Need for Layer 3 Switches.	53
15	Layer 4 Switching.	55
15a	Is it Hype or Hope ?	59
16	Performance Parameters in Layer 4 Switching.	61
16a	Packet Filtering and Prioritization.	61
16b	Load Balancing.	62
17	Switching operation at Layer 4.	65
18	Why is Layer 4 Switching Important ?	67

19	Benefits of Application Level Control in Layer 4 Switching. ..	*68*
19a	Application Level - Quality of Service (Qos).	*68*
19b	Application Level - Access Control (Security).	*69*
19c	Application Level - Accounting.	*70*
	RMON Groups.	*71*
20	Benefits of Layer 4 Switching.	*73*
21	Layer 5 Switching.	*75*
22	Need for Layer 5 Switching.	*76*
23	Objective of Layer 5 Switching.	*77*
24	Switching Operation at Layer 5.	*77*
25	Web Caching.	*79*
26	Concept Cycle behind Layer 5 Switching Strategy.	*83*
27	Web Traffic Scenarios.	*85*
27a	Authenticated/Non Encrypted HTTP based transactions.	*85*
	Persistence via Cookies.	*87*
	Prioritizing Services via Cookies.	*88*
27b	End-to-End Encrypted SSL based transactions.	*89*
	How SSL Technology works ?	*90*
27c	Authenticated/ Encrypted HTTP based transactions.	*91*
	HTTP/1.0 Protocol.	*92*
	Session Tracking Mechanisms.	*93*
	Server Persistence.	*94*
	Better Solution to Session Tracking - HTTP/1.1 Protocol.	*96*
28	Conclusion.	*97*
29	References.	*99*

M.S. - Thesis.

Thesis Topic: *Analyzing the costs/tradeoffs involved between layer 2, layer 3, layer 4 and layer 5 switching.*

Methodology: Researching resources from the web, journals and books.

Abstract: The switching function was primarily entrusted to Layer 2 of the OSI model, i.e. the Data Link Layer. A Layer 2 switch performs forwarding decisions by analyzing the MAC (Media Access Control) address of the destination segment in the frame. The Layer 2 switch checks for the destination address and transmits the packet to the appropriate segment if the address is present in its table of known destinations. If the entry for that address is not present, the switch then forwards the packet to all segments except the one on which it came from. This is known as flooding. When it gets a reply from the destination segment, it learns the location of the new address and adds it to its table of known destinations. As number of users are increasing on the network, the speed and the bandwidth of the network is being stretched to its limits. Earlier, switching was primarily entrusted to Layer 2 (Data Link Layer) of the OSI model, but now there are switches that operate at Layer 3 (Network Layer), Layer 4 (Transport Layer) and Layer 5 (Session Layer) of the OSI model. Going from one layer to the other layer does involve some costs/tradeoffs. My thesis explores the costs and tradeoffs involved with switching based on layers 2, 3, 4 and 5 of the OSI reference model.

Layer 2 Switching.

Local Area Networks have to deal with increased bandwidth problems as traffic on the networks is increasing day by day. More users are being added onto the network and as a result more stations are trying to gain access to the network. This slows the speed of the network considerably, and in peak time can completely congest the network services.

If the number of workstations on the network was the only problem, upgrading the backbone systems that connect the various LAN's could have solved it. Bridges and Routers could have been added to reduce the number of user's/workstations on each segment to an acceptable number. But in the past couple of years the processing capability of the workstations has grown five fold. Along with increase in processing capability of today's workstations, the demand for multimedia applications has also gone up. Multimedia applications take a lot of bandwidth off the network.

There has also been an increase in the use of Client-Server architecture model wherein the software rests within the server. The traffic between client and the server has gone up. This has increased the level of traffic on the network.

A possible solution to the overcome the bandwidth problem would be to install a fast network technology, e.g. replacing the traditional Ethernet with Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI) or Fast Ethernet. Although these technologies are really good, but its going to cost the organization a lot to migrate to such new technologies. New equipment/infrastructure and staff training will be required. Another way out could be to install bridges and routers on the network and segment the network into smaller parts. This scheme would only work if the traffic on the network is low, otherwise they would only act as network bottlenecks. LAN switching can be considered as a possible solution to this problem.

Reference: *LAN Switching.*
ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm

Introduction:

Switches like bridges, are data communication devices that operate at the layer 2 (Data Link Layer) of the OSI reference model and hence are known as data link layer devices. The LAN's (Local Area Networks) are becoming increasingly congested with greater and greater amounts of traffic due to an increase in the number of network users and coupled with the following factors there is constant stress on the network to provide for services.

- **Faster CPU's:** The most common desktop workstation is a PC. In the early eighties, majority of the PC's could execute 1 (MIPS) million instructions per second. But now PC's are coming with processing speeds upto 75 MIPS. A couple of such modern workstations can completely saturate the network.

  Reference: *http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs0./10.htm*

- **Multitasking Environment:** Multitasking gives users the ability to initiate multiple network transactions at the same time. The CPU gives an appearance of executing all programs at the same time, but actually it switches from one program to the other. Windows 95, NT, Amiga and Unix use pre-emptive multitasking in which the operating system sends CPU time slices for the programs, where as Microsoft 3.x and MultiFinder (for Macintosh) use co-operative multitasking in which each program can control the CPU for as long as it desires. Initiating multiple network transactions does put strain on the network.

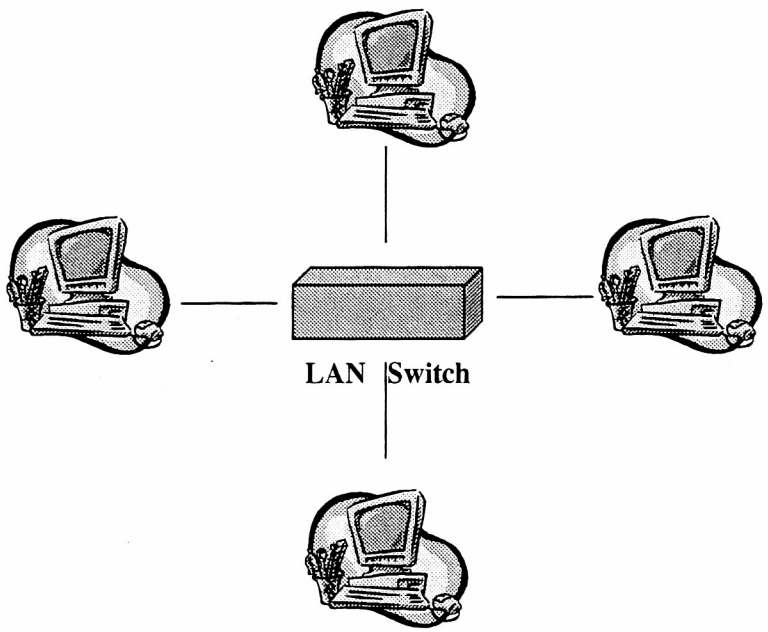
  Reference: *Multitasking.*
  http://www.pcwebopedia.com/TERM/M/multitasking.html
  Reference: *Multitasking.*
  http://burks.brighton.ac.uk/burks/foldoc/83/75.htm

- **Network Intensive applications:** The use of Client-Server applications is on the rise and the World Wide Web is increasingly being used. Client-Server applications

allow the administrators to centralize the information and thus make it easy to manage and protect the information. Client-Server architecture provides users with the capability of storing many of their applications and data on file servers instead on their PCs. With the kind of benefits the client server applications provide, the workplace will become even more network dependent in the future.

Reference: *Network Intensive Applications.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs0./10.htm

A LAN Switch is a Data-Link layer device.



Application
Presentation
Session
Transport
Network
Data-Link
Physical

Switching Basics:

The term Switching was earlier used to describe packet-switching technologies such as Link Access Procedure, Frame Relay, Switched Megabit Data Service (SMDS), and X.25. Now a day's Switching is referred to as a technology that is similar to a bridge in many ways.

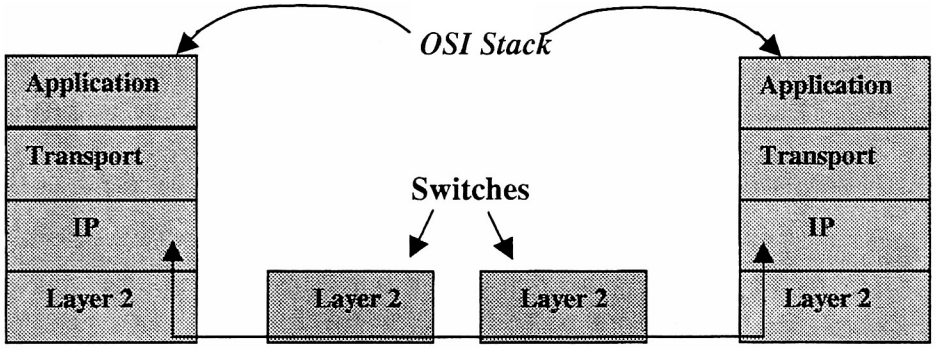
In Bridging, a device (known as a bridge) connects to two or more LAN segments. The bridge transmits the datagrams from one segment (known as the source), to the destination segment, which could be on the same or on a different segment. Bridge handles such a transfer of datagrams by analyzing their MAC (Media Access Control) address, through which it builds a table of known addresses. If the bridge notices that the destination of the datagram is on the same segment as the source it simply drops the datagram. If the destination is on a different segment, the bridge will transmit the datagram to that segment only. But if the destination address is not in its table of addresses it will transmit the datagram to all the ports except the port from which it came through. This process is also called flooding. The basic benefit of bridging is that it alleviates congestion by isolating the traffic to certain network segments only. Like bridges switches also connect LAN segments, use MAC addresses to determine the segment on which a datagram needs to be transmitted and also reduce traffic on the network.

Reference: *LAN Switching.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm

The most common LAN media is the traditional Ethernet, which has a capacity of 10Mbps, is a half-duplex technology. Each host on the network checks to see if there is any transmission of data. If the node senses any traffic it defers and waits for some time before it again checks the status of the line. If no other host is transmitting or the line is idle, it transmits data. Inspite of such kind of transmission deferral, two or more hosts can transmit at the same time, which can result in a collision. When such a situation occurs the hosts start back off algorithm. They have to wait for some more time before they can begin to transmit again. As more and more hosts are being added onto the network, they need to wait more often before they can transmit data and as a result there will always be

a greater probability of collisions as more hosts are trying to transmit data. An Ethernet LAN Switch improves the network bandwidth by separating collision domains.

The process of switching consists of two perspectives, Local and End-to-End. The local perspective deals with how the switch decides (upon receiving the packet), which output port it will switch the data frame through. In other words what information contained within the data frame, does the switch use to move frames coming from an input port to the output port. The second perspective deals with establishing a path between two endpoints maintained through a network of switches. This is known as switch path control.



Reference: *Switching Concepts and LAN Switching Technologies. - Layer 2 Switching in the Protocol Stack. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

Switch forwarding Techniques.

A switch is simply a box with a number of ports attached to it. Devices such as workstations, routers and other switches attach to these ports to forward the data. When a data frame arrives at a switch through the input port the job of the switch is to examine the frame and make a switching decision. The switch can either discard the frame if the

destination station happens to be on the same segment, or move it to the correct out port by conducting a table lookup of known destinations or send it to all stations except the port through which it came from (this is done when the destination station is not present in the table of known destinations). The switch is able to make such calculated decisions by analyzing the information that's contained in the data frame. The information analyzed by the switch within the data frame consists of one of the following:

1. *Destination Address.*
2. *Source-route Vector.*

Switching by Analyzing the Destination Address.

Switch transmits frames from the source to the destination segment by analyzing the MAC (Media Access Control) address in the frame. When a Switch receives a frame, it checks to see if the address exists in its table of known destinations. If the destination address is present in the table and is on the same segment, it simply drops the frame, as there is no need to transmit it further. This is based on the common assumption that the switch will not forward the frame through the same interface it came from.

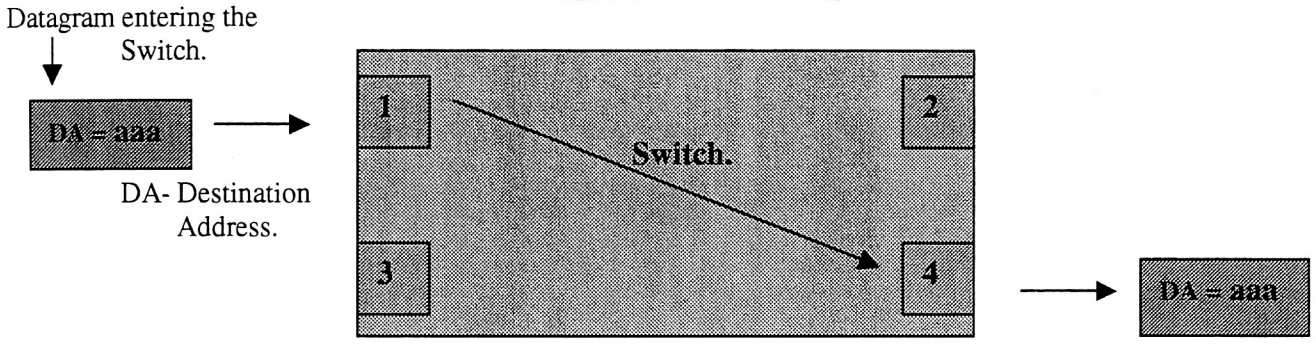
If the Switch knows that the destination is on a different segment it will transmit the frame to that segment only. In this way the Switch is able to reduce congestion on the network.

If the address is not present in its table of known destinations, the Switch will transmit the frame on all segments except the one on which it came from (this technique is known as flooding). Switches also connect LAN segments, use MAC addresses to make forwarding decisions and thereby reduce congestion on the network.

Reference: *Switching by Analyzing the Destination Address.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm#xtocid191881

Data forwarding operation by the switch.

Destination Address	Port
aaa	**4**
bbb	2
ccc	3
ddd	1



Reference: *Switching Concepts and LAN Switching Technologies. - Switching by Analyzing the Destination Address. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

In the following diagram, the switch receives a data frame. As soon as it gets the data frame it analyzes the destination address by doing a lookup for that address in its table and finding the corresponding port number. The destination address "aaa" has "4" as the corresponding output port number. It then sends the data frame out through port number"4".

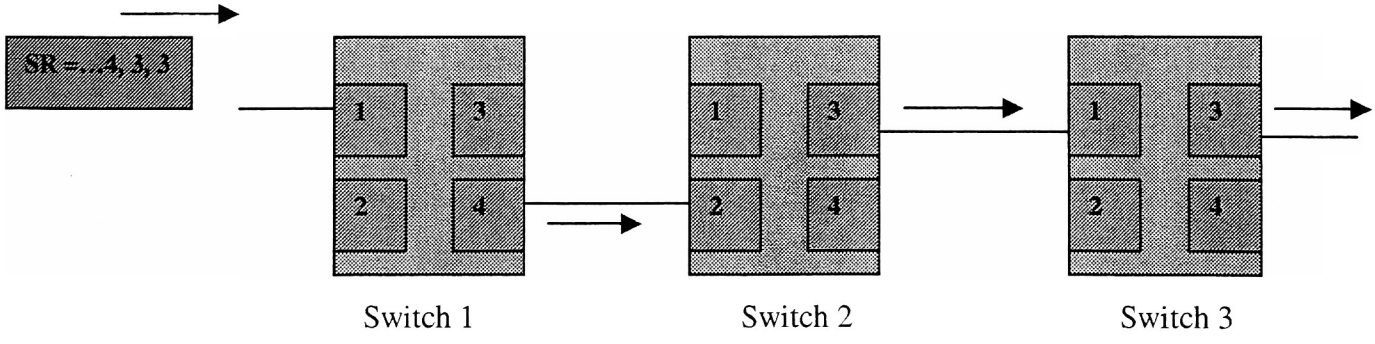
Switching by analyzing the Source-Route vector.

Source-route vector is another technique used by the switch to make a forwarding decision. The source-route vector sequence is contained within the frame and consists of

a sequence of elements that the data frame needs to traverse through before it can reach the destination station. This sequence of elements in the source-route vector can range from the output port numbers on the switch to the addresses of the switch along the path. Switching by analyzing the source-route vector does not involve maintaining an address table of known destinations as in the case of switching by analyzing the destination address.

The source-route vector is inserted into the frame and the switch uses this information to forward the frame through the appropriate output port. Although this does involve a substantial amount of work (gather information on the sequence of elements – needed to assemble an accurate source-route vector.) on part of the sender, source-route switching is an efficient way of forwarding the data frame to its destination station.

SR – Source Route.



Reference: *Switching Concepts and LAN Switching Technologies. - Switching by analyzing the Source-Route vector. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

In the following diagram the switch receives a data frame which has a source-route vector ***(SR)*** inserted into it by the sender. As soon as the first switch receives the frame it accesses the source-route information and makes an informed decision based on the

source-route. As per the source-route information, Switch 1 sends the frame through port 4. Switch 2 in turn sends it out through port 3 and so on.

Switch Path Control.

The data forwarding techniques that have been discussed earlier i.e. switching by analyzing the destination address and switching by analyzing the source-route vector, need some sort of path control in order to create and maintain information in the switch so that the data frames can be forwarded to their correct destination.

Switch path control involves an exchange of control messages between the switches on the network, in order to establish a consistent set of switch forwarding tables. Switch path control is established through one of the following mechanisms.

1. *Address learning.*
2. *Spanning tree Algorithm.*
3. *Broadcast and Re-discover.*
4. *Link state routing.*
5. *Explicit signaling.*

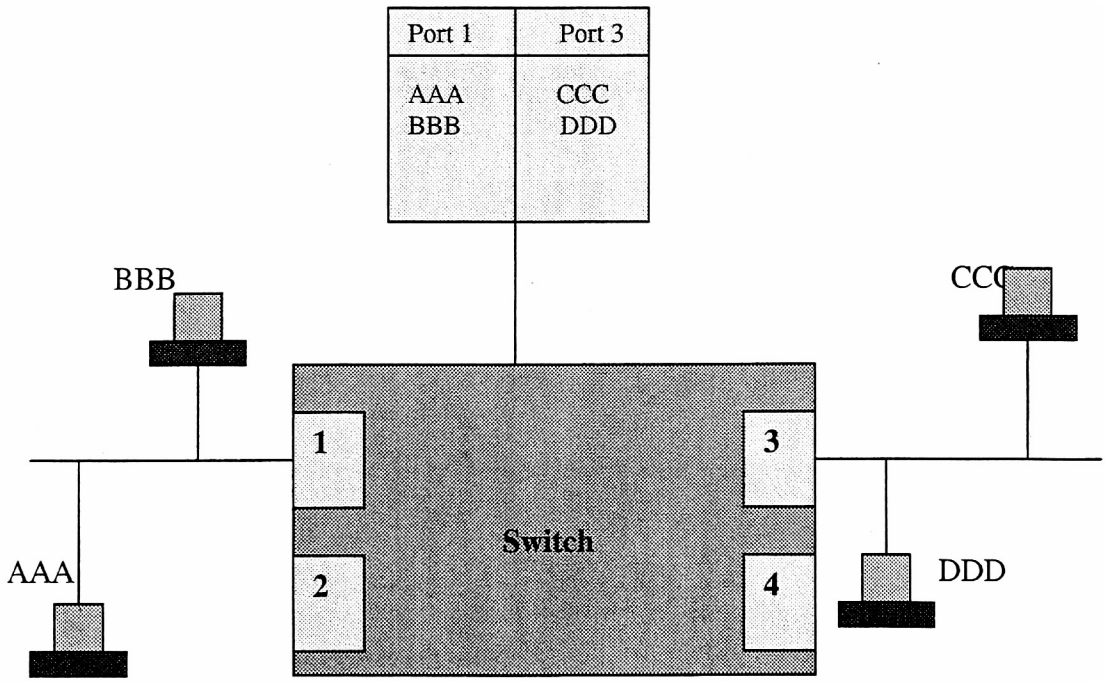
***Reference**: Switching Concepts and LAN Switching Technologies. - Switch Path Control. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

Address learning.

Address learning is one of the simplest techniques that the switch uses to build and maintain a switch-forwarding table. This table is used to forward the frames to their correct destination. This process involves taking an incoming frame from one interface/source and sending it to the desired interface/destination. In the case of Layer 2 switches, the frames are forwarded to their destination based on the MAC (Media Access

Control) address that's contained inside the frame. As soon as the frame comes up to the switch, the switch looks at the MAC address and checks to see in its Arp table if it has an entry associated for that particular destination address. If the entry for the destination address is found, the switch forwards the frame to that particular segment only. In this way the switch preserves the network and bandwidth utilization. But if the switch encounters a MAC address that is not present in its Arp table, it sends the frame to all the ports except the port from which it came from. This process of broadcasting the frame is known as flooding. When the frame's reply is returned, the switch learns the location of the destination station and quickly updates its address table. The next time a frame is forwarded to the same destination, the switch will send the frame to that segment only rather than sending it to all the segments.

Reference: *Address learning.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm.

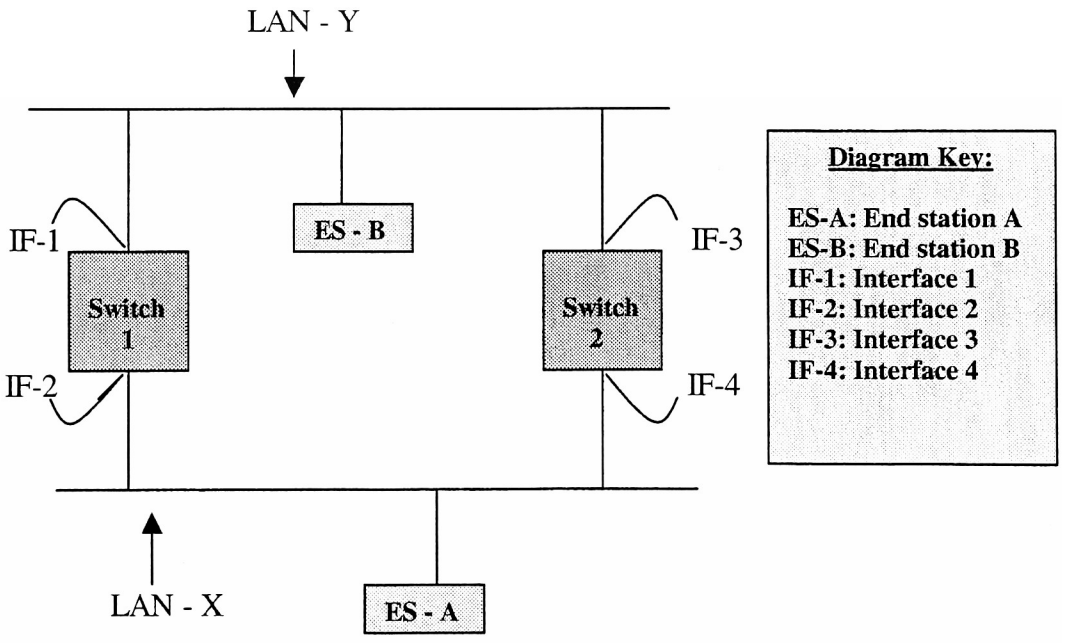


Reference: *Switching Concepts and LAN Switching Technologies. - Address learning. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

As it is evident from the above diagram, the switch analyzes the destination address and the associated port entry in its table of known destinations. It then forwards the frame through the appropriate port.

Spanning Tree Algorithm.

Loops within the network can form if there is more than one path between the source and the destination station. If there is a loop in the network, bridges may forward traffic indefinitely, which can result in increased traffic and degradation in network performance. This can lead to corruption in the switching table and inefficient use of network bandwidth. To get around the problem of looping on the network, switches implement the spanning tree algorithm. Spanning tree algorithm ensures the existence of a loop-free topology in networks that contain parallel bridges.



Reference: *Solution to loops in a network.*
http://support.baynetworks.com/library/tpubs/html/router/soft1000/bridge/2950A-19.html

The following figure shows an example of a network loop, taking place in a parallel bridge topology (Switch 1 and Switch 2). When the end station-A (ES-A) sends a frame

to end station–B (ES-B), both Switch 1 and Switch 2 receive the frame. Since this is the first frame sent between the 2 end stations there are no forwarding entries in their switching tables. Both the Switches receive the frame and update their tables to indicate that end station-A is in the direction of LAN-X. Both the Switches flood the entry through the entire network except the port from which it came from. Switch 1 forwards the frame through interface 1 (IF-1), and Switch 2 forwards the frame through interface 3 (IF-3). As the same frame is forwarded through two different Switches, end station B (ES-B) receives two copies of the same frame. The frame forwarded by Switch 1 through interface 1 (IF-1) not only reaches end station B, but also to Switch 2 via interface 3 (IF-3). Similarly, the frame forwarded by Switch 2 through interface 3 (IF-3), reaches Switch 1 via interface 1 (IF1). Both the Switches update their forwarding table to indicate that the frame came from LAN-Y, and that the end station A (ES-A) is in direction of LAN-Y. The Switch tables are now corrupted, and neither Switch can properly forward the frame to end station B (ES-B).

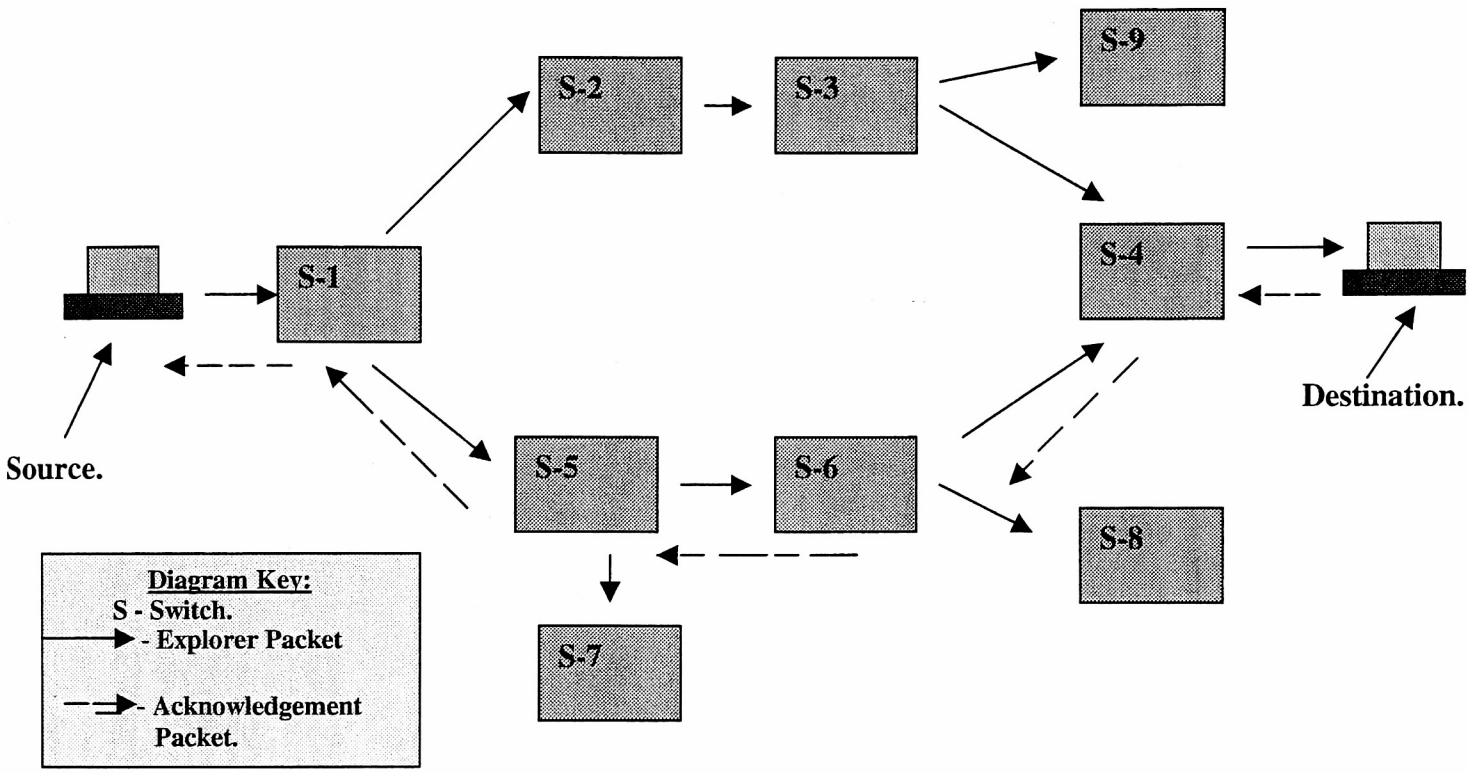
This problem can be avoided by implementing the spanning tree algorithm, which results in a single path between two end stations on an extended network. Spanning Tree is a protocol, which allows bridges to connect two or more of the same segments and maintain a single active path. It allows the network to automatically reconfigure itself if there is a bridge/data path failure.

Reference: *Spanning Tree Algorithm.*
http://support.baynetworks.com/library/tpubs/html/router/soft1000/bridge/2950A-19.html
Reference: *Spanning Tree Algorithm.*
http://www.ciscoworldmagazine.com/monthly/1999/12/spantree.shtml

Broadcast and discover.

Broadcast and discover is another technique used in LAN switching to locate a switched path on the network. The idea out here is to explore for one or more paths to the

destination station, by sending a broadcast explorer frame. Once the destination station receives this frame it sends back the frame to the source station with a source-route vector inserted inside the frame. The source station can then use the information contained inside the source-route vector to forward all frames to the destination station.



Reference: *Switching Concepts and LAN Switching Technologies. - Broadcast and Discover. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

The source station floods the entire network with the explorer frame (represented by a bold arrow line). The destination station upon receiving the explorer frame sends an acknowledgement frame (represented by a dotted line) to the source station using the source-route (4,6,5,1). The sender will now use this path if it needs to send frames to the destination station.

Link State routing.

This technique of switch path control assumes that switches are running link state routing protocol. The switches exchange link state information with their neighboring

switches and create a link state table/database, which is used to forward the packets to the destination station. Whenever there is a change in the network topology, i.e. a change in link status (goes up or down), a notification, called the *link state advertisement* (LSA) is flooded throughout the entire network. All the switches on the network note the change in their respective tables, and recompute their routes accordingly. Link State routing is far superior to the distance vector routing protocols such as RIP, which uses hop count as a criterion for forwarding the packets. Link state routing protocols (such as OSPF) use other metrics such as, link speeds, and traffic congestion, apart from hop count to forward the packets to the destination station. Link state routing also minimizes overhead packet traffic when announcing changes, by only sending information relating to the change, and not the entire routing table. This saves a lot of bandwidth on the network.

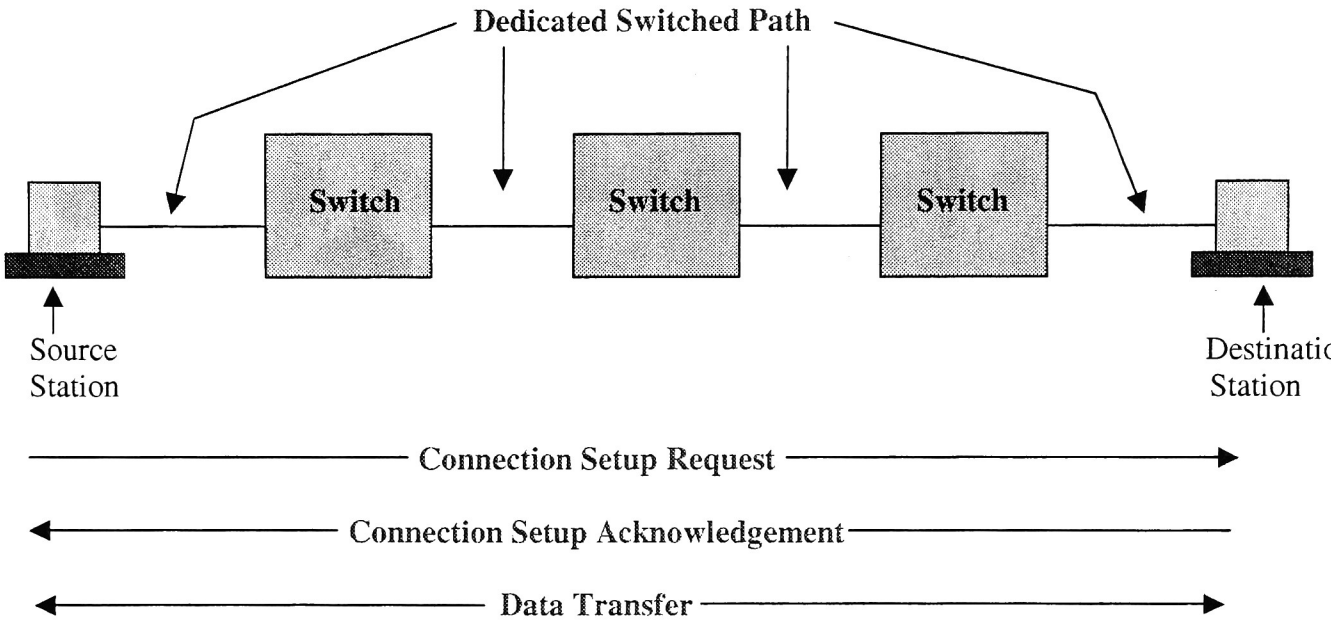
Reference: *Link State Routing Protocols.*
http://www.freesoft.org/CIE/Topics/118.htm
Reference: *Link State Routing Protocols.*
http://burks.brighton.ac.uk/burks/foldoc/8/67.htm
Reference: *Overview of common routing protocols. - Link State Routing Protocols.*
http://www.wireless-nets.com/whitepaper_routing.htm

Explicit Signaling.

Explicit Signaling is another way to establish a switched path. For explicit signaling to work, a dedicated switched path is established between the source and the destination station. To establish a dedicated switched path, the source station sends a connection setup request message to the destination station. The purpose of sending this frame is to ensure that the path is active and that it will be able to handle the data traffic. The source station can begin the flow of traffic to the destination station, when it receives an acknowledgement from the destination station confirming that the path has sufficient

capacity to handle the data traffic. The mechanism of explicit signaling is detailed in the following diagram: -

Explicit Signaling.



Explicit signaling has advantages and disadvantages associated with it. On the upside, explicit signaling can confirm that there is a dedicated path to the destination station before transfer of data can actually begin. The source station does not need to send frames to the destination station and wait for an acknowledgement, and then when no acknowledgement is received, decide that the destination station is unreachable.

Another benefit through explicit signaling is that route calculation is performed only once through the entire data flow. The route/switched path is determined before the flow of data frames starts between the source and the destination. This is done by the source station, sending a connection setup request to the destination station and receiving a connection setup acknowledgement response in return. This saves a lot of time as route calculation is done only once and not at each network interface between the source and

the destination station. Cost metrics such as bandwidth and delay can also be communicated into the network and processed by each switch along the switched path. Such a technique produces a switched path that meets the bandwidth and delay characteristics of the data flow between the source and the destination station as required.

Reference: *Switching Concepts and LAN Switching Technologies. - Explicit Signaling*
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

The Layer 2 Switching process.

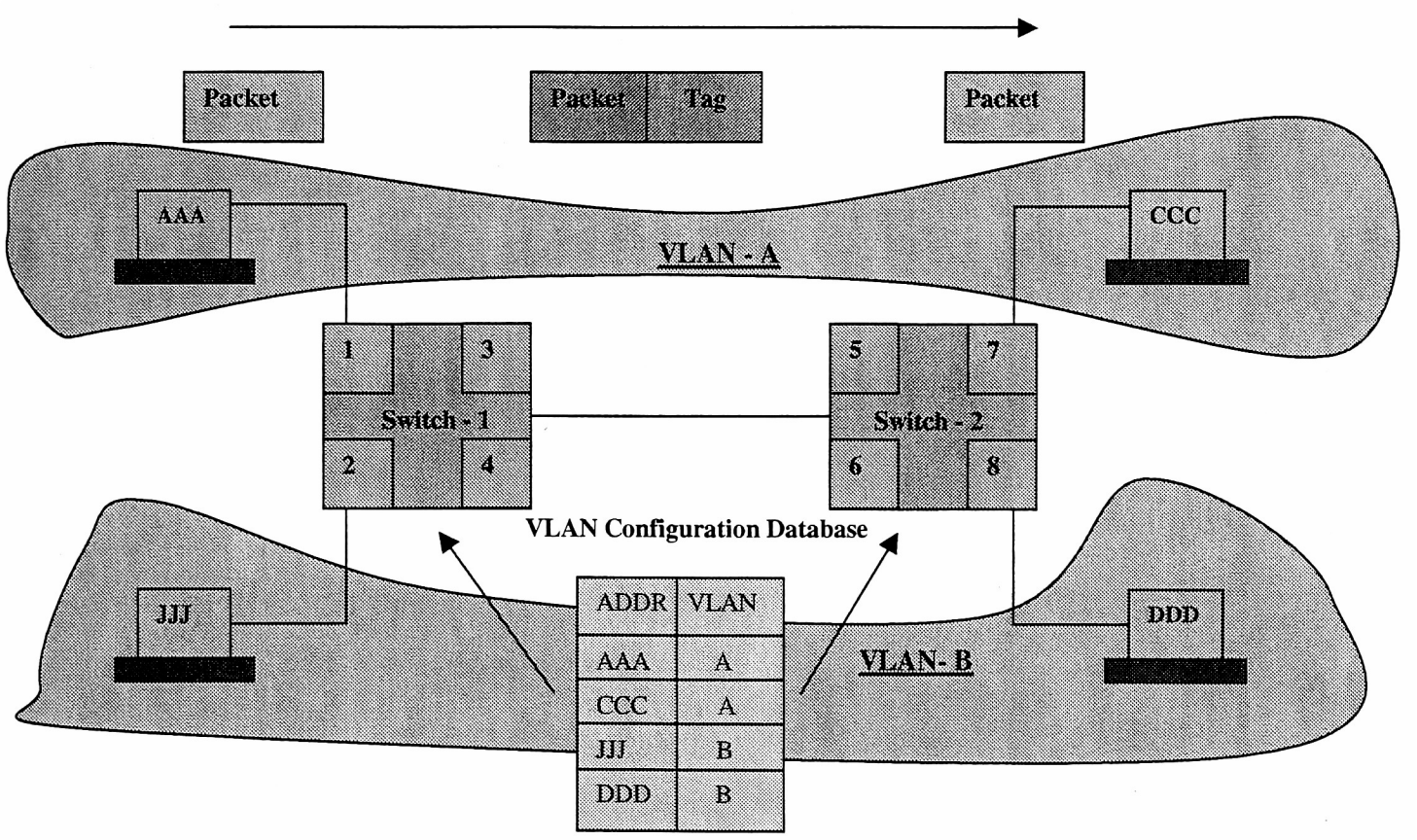
The layer 2 switching process comprises of a couple of separate processes that help the switch in creating/maintaining a switching table and forwarding the frames to their destination.

1. *The Ingress Rules.*
2. *Learning process.*
3. *Forwarding process.*

The Ingress Rule.

When a frame arrives at the input port, the Ingress rules for the port check for the VLAN (Virtual LAN) tags in the frame to determine whether the frame will be discarded or sent to the leaming process. The first check out here is to see if the field ' Acceptable Frame Types ' is set to Admit all frames or Admit Only VLAN tagged frames. A port that transmits only VLAN tagged frames, irrespective of whichever VLAN it belongs to, will have the field: - Acceptable Frame Types set to Admit Only VLAN tagged frames. Every frame that is received by the switch is to be associated with a particular VLAN. Every port of the switch is associated with one or more VLAN's, and therefore every incoming frame needs to have a VLAN identifier (VID) to show which VLAN it belongs to. This way the switches have a methodology in place to identify and forward the frames

to the correct VLAN. As soon as the ingress switch port receives a frame, some portion of the frame's contents are compared and examined against the VLAN configuration database. A tag or VLAN identifier (VID) is then inserted into the frame. The VLAN switch uses the VID and the corresponding destination address to forward the frame to the correct VLAN destination.



As it is depicted from the above diagram, Switches 1 and 2 have been configured to have *VLAN – A* with workstations AAA & CCC, and *VLAN – B* with workstations JJJ & DDD. The VLAN Configuration Database information is distributed to every switch that might be a member of either of these VLAN's. The switch ports can learn this information through either static or a dynamic learning process.

Out here in the diagram, station AAA sends a frame destined for station CCC. Switch – 1 receives the frame through port 1, which looks up into the VLAN Configuration Database, and finds that station AAA is a member of VLAN- A. It then appends a tag to the frame and sends it to station CCC. As soon as the frame arrives at Switch – 2, it checks the VLAN tag and finds that the frame belongs to VLAN – A. It then removes the tag and forwards the frame to station CCC through port 7.

Reference: *Layer 2 Switching process.*
http://www.alliedtelesyn.co.nz/support/rapier/rapier221/switch.pdf
Reference: *Switching Concepts and LAN Switching Technologies. – Virtual LAN's.*
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

Learning process.

As soon as the frame enters the switch, its source MAC address is analyzed with the entries in the forwarding database, which is maintained by the switch. This forwarding database contains an entry for every unique station the switch knows about on the network. If the source address is not present in the database the switch quickly updates its database with the entry.

Process to update its database: - if the switch encounters a MAC address that is not present in its Arp table, it sends the frame to all the ports except the port from which it came from. This process of broadcasting the frame is known as flooding. When the frame's reply is returned, the switch leams the location of the destination station and quickly updates its address table. The next time a frame is forwarded to the same destination, the switch will send the frame to that segment only rather than sending it to all the segments. After the table has been updated with the new entry, the switch starts an ageing timer for that entry. On the contrary if the source address is already present in the database the ageing timer is restarted. By default switch learning is enabled, which helps

the switch in building up its database. The switch learning can be enabled or disabled by giving the following commands: -

ENABLE SWITCH LEARNING.

DISABLE SWITCH LEARNING.

The switch also checks for the ageing timer entry in the database. If this entry expires before the switch receives another frame with the same source address, the entry is removed from the database. This ensures that the forwarding database contains up to date information about stations that are inactive or have been taken off from the network. As in the case of switch learning, the ageing timer is also by default enabled. The timer can be enabled or disabled by giving the following commands: -

ENABLE SWITCH AGEINGTIMER.

DISABLE SWITCH AGEINGTIMER.

The default value for the ageing timer is set to 300 seconds (5 minutes), but can be modified to change the timer value by giving the following command: -

SET SWITCH AGEINGTIMER.

Reference: *Layer 2 Switching process.*
http://www.alliedtelesyn.co.nz/support/rapier/rapier221/switch.pdf

Forwarding process.

As soon as the frame reaches the switch, the destination address contained in the frame is compared with the entries in the switching table for a possible match. If the switch finds the destination address to be on the same segment it simply discards the frame and does not forward it.

If the switch cannot find a possible match for the destination address in its forwarding table, it floods the frame through the entire network except the port through which it came from. Upon receiving an acknowledgement from the destination station the

switch quickly updates its table. If the destination address is found, the switch forwards the frame to that segment only, thereby preserving the bandwidth and reducing traffic on the network.

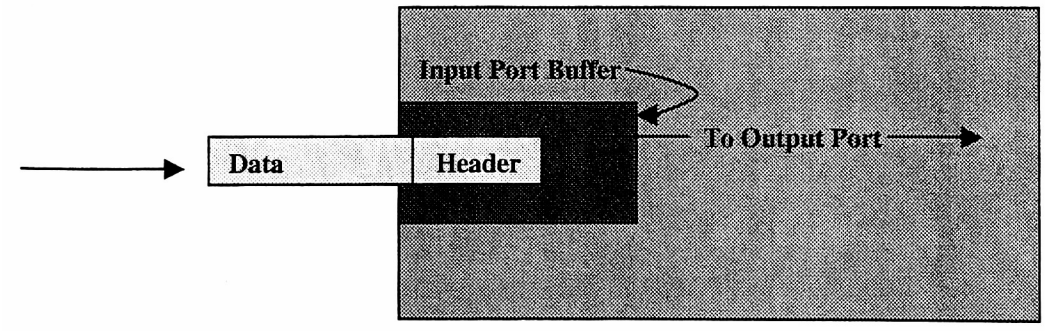
Reference: *Forwarding process.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm.

The process of switching is to take the frame from the input port and send it through the correct output port. A LAN switch can forward the frame using any of the two forwarding techniques: -

1. *Cut through switching.*
2. *Store and forward switching.*

Switches using ***Cut through switching*** begin transmission of the frame even before the entire frame is received. Forwarding of the first part of the frame can begin even as the remaining part of the frame is being read into the input port switch buffer. The benefit of using such kind of forwarding technique is lower transmission latency, which can prove useful when supporting delay-sensitive traffic. The disadvantage of using such a technique is that no CRC (Cyclic Redundancy Check) is done in these switches. The frames, whether valid or invalid are transmitted to the output port.

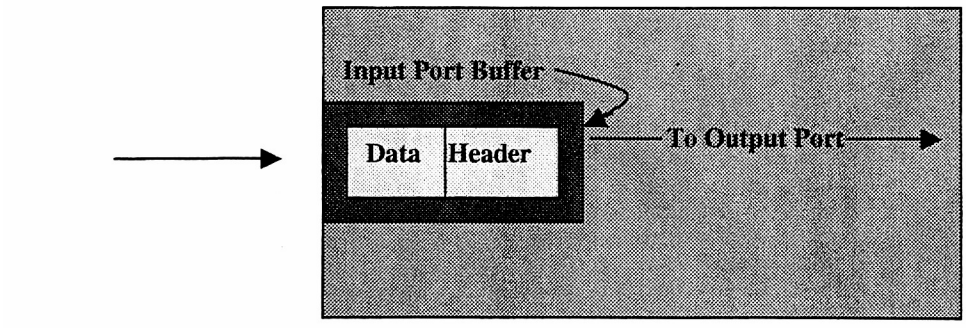
Switch Port.



Reference: *Cut Through Switching.*
ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm#cut
Reference: *Cut Through Switching.*
http://www.anixter.com/techlib/whiteppr/network/d0504p06.htm
Reference: *Switching Concepts and LAN Switching Technologies. - Cut Through Switching. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

Store and forward switching is another kind of forwarding mechanism that the LAN switches use to forward the frames to the destination station. As soon as the switch receives the frame, it reads the entire frame into a buffer before deciding where to send it. When the entire frame has arrived, a CRC (Cyclic Redundancy Check) is done on the frame to check for any errors. If the frame fails the CRC, the switch can discard the frame without forwarding it to the next segment or switch. If the frame passes the CRC, the switch forwards the frame through the correct output port. Performing CRC on the entire frame can increase latency. Although there are disadvantages in using Store and Forward switching mechanism, in some cases it is essential. Frames buffered in the memory till they are fully received, although adds latency, but reduces the probability of sending bad frames to the destination station.

Switch Port.



Reference: *Store and forward switching.*
ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm#cut
Reference: *Store and forward switching.*
http://www.anixter.com/techlib/whiteppr/network/d0504p06.htm

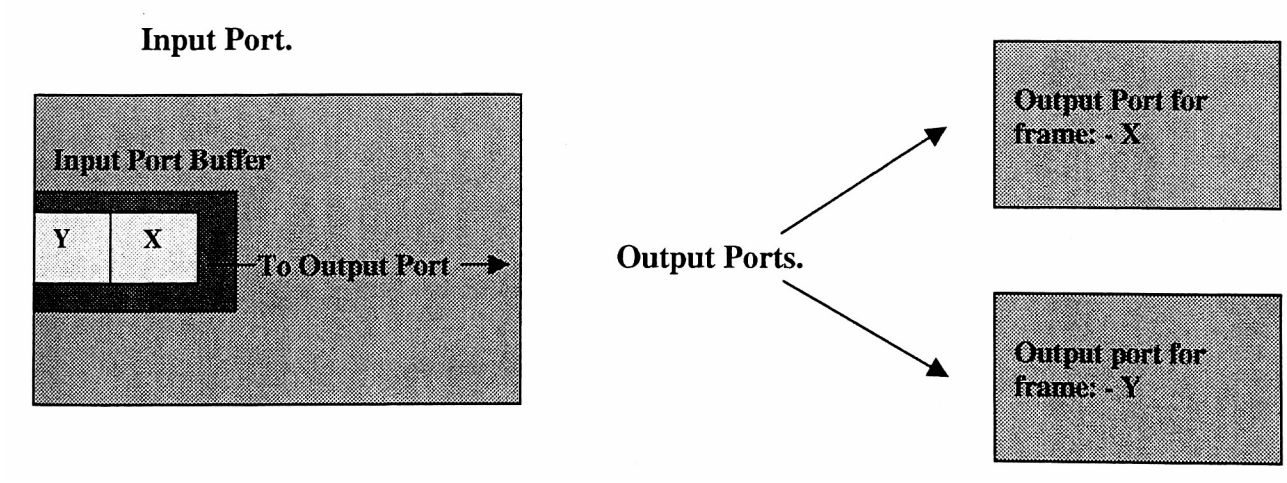
Reference: *Switching Concepts and LAN Switching Technologies. - Store and forward switching. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.*

Types of Buffering.

As discussed above in Store and Forward switching, the frames are buffered in the memory before they are forwarded to their destination. Buffering can be of two types: -

1. *Input Buffering.*
2. *Output Buffering.*

During ***Input buffering,*** the frames are buffered at the input ports. The incoming frame is stored in the buffer as soon at it reaches the switch. This technique is beneficial in situations when more than one port is trying to send frames to the same output port. Frames are buffered in the memory and forwarded only when the destination port is free. A problem might occur when the frames have to be sent to more than one destination port.



Lets assume that output port for frame X is busy. Frame X occupies the top slot in the input port buffer. Even though the output port for frame Y may be free, it'll still have to

wait for frame X to go to its destination port. Such a scenario is called head-of-line blocking. The problem of head-of-line blocking can be solved through ***output buffering***. During output buffering the frames can be forwarded to the output buffer even though it might be busy. Output buffer is useful when traffic to a destination port is heavy.

Reference: *Input and Output Buffering.*
ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm#buffer
Reference: *Switching Concepts and LAN Switching Technologies. - Input and Output Buffering*
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

Functions of Layer 2 Switching.

- **Address learning:** The Layer 2 switch retains in its filter table, the frame's source hardware address and the port interface it was received on. This helps the switch to forward frames in a much efficient manner.
- **Forward/Filter decisions:** As soon as the frame reaches the switch, the destination address contained in the frame is compared with the entries in the switching table for a possible match. If the switch cannot find a possible match for the destination address in its forwarding table, it floods the frame through the entire network except the port through which it came from. This process is known as flooding.
- **Loop Avoidance:** If multiple paths exist for the destination stations, network loops can occur. Spanning Tree Protocol is used to correct this problem, while still allowing redundancy.

Reference: *Layer 2 Switching.*
http://www.certifyexpress.com/cisc/resources/2switching.shtml

Benefits of Layer 2 Switching.

A switch performing its services at Layer 2 (Data Link Layer) of the OSI model offers the following benefits: -

- **Bandwidth:** The LAN switches provide good performance for the individual users that are logged on by providing the dedicated bandwidth to each switch port. This improves the network performance to a great extent. This technique of making a switch port represent a different network segment so as to get the dedicated network bandwidth is known as micro segmenting.
- **VLANs:** Switches at Layer 2 (Data Link Layer) have the ability to group different ports into one logical work group known as VLANs (Virtual LANs). Through this they can segment the workgroups traffic just to that domain. A virtual LAN (VLAN) is basically a group of hosts/network devices that form a single bridging domain. The basic purpose of forming a VLAN is to group related users irrespective of the physical connection of their host on the network. These users could be spread out on a campus network or could be geographically dispersed. If network devices such as routers can be excluded from this arrangement, users who are outside the domain cannot communicate with the people who form a part of the domain. This aspect is critical for sensitive projects and applications.
- **Network Management:** The software that's there on the switch allows the possibility to add users in the VLAN and later re-assign them. Re-cabling to change the connectivity is no longer required as the software that is installed in the switch reconfigures the LAN logically in a matter of a few seconds.

Reference: *Benefits of Layer 2 Switching.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm

Layer 3 Switching.

Layer 3 Switching is a form of traditional routing, i.e. switching the traffic between IP subnets. It attempts to reduce the problems/bottlenecks that are associated with the traditional routers. Traditionally, routing was used to improve the network performance in areas where bandwidth was a problem. Routers would prioritize traffic on congested interfaces so as to guarantee the performance of important applications. Routers have also been used to isolate traffic (*e.g. application of access lists on router interfaces.*) on the networks in order to improve their performance and also prevent broadcasts from flooding the network.

The backbone of the Internet and that of many large organizations is built upon the foundation of layer 3 of the OSI model, i.e. the Network Layer. IP is the premier protocol for layer 3. Majority of the organizations seemed to benefit from changing routed and shared networks towards layer 2 switches, but partitioning to a certain degree was required. And as a result, routers were maintained at many points within the network of the organization. As long as the data traffic remained within the local subnet of the organization there weren't any bottlenecks or problems, as the data was being serviced through the layer 2 switches.

With the ever-increasing acceptance of the layer 2 switches other developments were taking place. Intranets (organization wide client/server communication based upon the Web technology) were being deployed. This began the movement of data off the local subnet of the organization to the routed network, and consequently the shortcomings of router performance were being felt. With routers causing problems in transfer of data, organizations were increasingly reluctant in deploying newer technologies. The router vendors were asked to increase the performance of the routers, and they did come up with high performance interface cards, but this aspect did not attack the throughput problem as

the throughput was directly linked to the basic software architecture, which could not go any faster. The same software that was being used to manage the WAN (Wide Area Network) links, X.25 and the asynchronous terminal lines had to handle the gigabit networks. This meant additional strain on the network.

At the same time, work was being done by entities such as the ATM forum to reduce the problems associated with Layer 3 by utilizing the capabilities of lower layers. One such result from the work being done was the Multiprotocol over ATM (MPOA) specification that uses the Layer 3 information and IETF's NHRP protocol to offload the routers and provide the forwarding function at the physical layer. The layer 3 switch can route at Layer 3 / use the Multiprotocol over ATM. In both respects the performance is completely identical. A layer 3 switch does almost everything that a traditional router does.

Working aspects of a layer 3 switch: -

- Analyses the path to be used to forward the packet based on Layer 3 (Network Layer) information.
- Does a CRC check to validate the integrity of the header.
- Checks on the expiration of packets and updates them accordingly.

***Reference**: Layer 3 switching.*
http://www.pulsewan.com/data101/layer3_switching_basics.htm

Layer 3 Switching has become immensely popular in the networking circles. It represents a technology that is destined to replace the traditional router. Actually it's a class of a high performance switched router, capable of handling millions of packets per second, thereby increasing the overall network effectiveness. The job of a switch

is to examine the incoming packet, extract the destination address, lookout for the destination address in its table of known addresses, re-write the packet control data and send the packet through the appropriate interface for transmission. The performance of a switch can be gauged from how fast it is able to transmit the packet to the destination station over a fixed period of time. The faster the packets arrive, the faster they need to be transmitted. There would be congestion in the network and loss in performance if there were a lag between receiving and transmitting a packet.

***Reference**: Layer 3 Switching. Re-Inventing the Router. The Technology Guide Series at techguide.com. http://www.techguide.com/html/3switch.pdf*

When discussing Layer 3 Switching, the prime area of our focus is its raw performance, which refers to the number of packets the Layer 3 Switch can process over a fixed period of time. Layer 3 Switches have the capability to process millions of packets per second (pps) as compared to the traditional routers, which have evolved from a hundred thousand packets per second to a million packets per second. Routers and the Layer 3 Switches have lot of similarities. These similarities are not just restricted to the Packet Switching methods but also to route processing and management, and intelligent network services.

- **Packet Switching:** Switching of packets is the simplest operation in a layer 3 switch. The only major difference between the packet switching operation of a Layer 3 Switch and a router is in the physical implementation. In routers, packet switching takes place in microprocessor-based engines, whereas a Layer 3 Switch uses ASIC Hardware (Application Specific Integrated Circuit). With such hardware in place, Layer 3 Switches can achieve forwarding rates that are much higher as compared to

the forwarding operation within a router. Apart from forwarding, the switching engine also does the following activities:

1. Packet Manipulation by creating an Ethernet frame with its own MAC (Media Access Control) address.
2. Decrementing the TTL (Time to Live) field in the IP header.
3. Recalculating the FCS (Frame Check Sequence)
4. Ability to perform the longest IP address look up

This process is repeated time and again for each packet that comes to the switch, and hence the name "Packet Switching".

Reference: *The key to greater performance and application control - Packet switching.* *http://www.enterasys.com/products/whitepapers/multilayer/*

Layer 3 Switching is not just about taking the comparative advantage of processing millions of packets per second. One needs to fully realize when to take the advantage of such a high performance technology. A common tendency is to get confused between the aggregate performance and the speed of the applications. If the network demand is in the order of ten thousand packets per second, and a Layer 3 Switch is introduced into the network that has a forwarding capability of 300,000 packets per second, such an arrangement will not have any impact on the network (or in other words will not speed up the applications). The most important aspects to be considered are *Route Processing and management, Intelligent Network Services, and Management and Security issues.*

- **Route Processing and Management:** Every Layer 3 node, whether Switch or a Router must be able to create a Routing table and be able to update the table

automatically with the constant changes taking place in the network topology. Changes to the network topology could be caused by link/device failures and additions or deletions to the network (change in network topology). These changes have to be taken into account when updates are made to the routing table. Routing tables are initialized before the flow of traffic begins on the network and must be kept synchronized with the changes taking place in the network. This is extremely essential for Route Management on the network.

In a large network, the number of routes and the events that can affect the routes are many and as a result, any change that takes place on the network needs to be reflected extremely fast in the routing table. Internet is a glaring example of a network that can take routing protocols to their limits. This is also true in case of high-speed networks. Updates to routing tables if not done quickly can seriously affect the performance of the network.

***Reference**: Layer 3 Switching. Re-Inventing the Router. The Technology Guide Series at techguide.com. http://www.techguide.com/html/3switch.pdf*

A number of dynamic routing protocols have been developed that need to be supported by the Layer 3 Switch. These include (RIP) Routing Information Protocol, the first dynamic routing protocol to be deployed. RIP is a distance vector protocol. But there were shortcomings to this protocol. Firstly there was slow convergence around failed links (in the order of minutes) and secondly it had limited scalability due to a finite hop count. (15 as a max). If a packet could not be delivered in 15 hops, the packet was discarded and the destination station was considered unreachable. It could not be deployed in big networks. Although RIP 2 was introduced, it did not overcome the limitations of RIP1.

Reference: *TCP/IP Protocol Suite - Routing Information Protocol.*
http://www.networksorcery.com/enp/protocol/rip.htm

In response to the shortcomings of RIP (Routing Information Protocol), other alternative routing protocols such as IGRP (Interior Gateway Routing Protocol) and OSPF (Open Shortest path First) were introduced. IGRP was introduced by Cisco to address the shortcomings of RIP.

IGRP provides greater degree of flexibility in determining the route that the packets will take through the network. Internetwork delay, bandwidth, reliability, and load are all taken in to account while making the routing decision. IGRP also permits multi-path routing. Dual equal-bandwidth lines can run a single stream of traffic, with automatic switchover to the second line if the first line goes down due to some reason. Multiple paths can also be used even if the metrics for the paths are different. If one path is three times better because its metric is three times lower than the other path, the better path will be used three times as often.

Reference: *IGRP Protocol Characteristics.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

To address the needs of their customers using IGRP as their routing protocol, Cisco developed Enhanced IGRP (EIGRP), which had the simplicity of IGRP and the benefit of fast convergence as that of OSPF.

OSPF (Open Shortest Path First), a link state routing protocol, is similar to the *Interior Gateway Routing Protocol* (IGRP). It was created because the *Routing Information Protocol* (RIP) was unable to serve large, heterogeneous internet-works. OSPF has the capability of faster convergence as compared to RIP, but is a complex protocol.

Reference: *OSPF (Open Shortest Path First) Background.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm#17394

Support for different routing protocols is the basic requirement for any Layer 3 Switch. In today's networking environment many protocols are in use. In this multi-protocol environment different route-processing subsystems need to co-operate with each other in order to ensure complete optimization of resources and minimal degree of conflicts in the network. The ability to jointly access and utilize different protocols suites allows the network administrator to develop a network to suit his/her needs. Its the routing protocols, the central nervous system of the Layer 3 switch that makes the Internet and Intranets work and ensures the stability and health of the network.

Reference: *Cisco Layer 3 Switching Demystified.*
http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/l3c85_wp.htm

- **Intelligent Network Services:** There is more to the internetworking requirement than just the ability to forward packets to their destination using the most optimal route/path. It's the intelligent network services that enables the network to remain up and healthy all the time and supports day-to-day operations. A few examples of this type of service include the following: -

a) The intelligent network services enable the deployment of mission critical applications such as SAP, BAAN, Oracle etc. Mere deployment of such mission critical applications is not enough. The network design needs to be such that there is perfect coordination amongst the network elements in solving the problems. One such tool is the **Hot Standby Router Protocol (HSRP)**, which provides redundancy for

the IP networks and ensures that user traffic recovers immediately from the first hop failure in the network.

Reference: *Cisco Layer 3 Switching Demystified*
http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/l3c85_wp.htm

Hot Standby Router Protocol (HSRP) provides a mechanism that is designed to support fail over of IP traffic on the network. The protocol protects against failure of the first hop router, when the source station can't learn the IP address of the first hop router dynamically. There are a couple of dynamic router discovery mechanisms available to the hosts to find such network information.

(1) ***Proxy Address Resolution Protocol:*** When a user (oz) on the network runs a proxy ARP, it basically sends an ARP request for the IP address of the remote host (for e.g. Router X) it wants to contact. On getting the ARP request from the user (oz), Router X responds on behalf of the remote host by providing its MAC (Media Access Control) address. *Now if the Router X goes down, the user would still keep on transmitting the data packets for that remote host to the MAC address of Router X.* Although the user can wait for convergence to take place on the network, the user will not be able to carry on with the data transmission till the time another router takes charge of the transmission.

(2) ***Dynamic Routing Protocol:*** Some IP hosts run Dynamic Routing Protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) on the network to find out which routers can be used. The disadvantage of using RIP is that it is slow in taking into account the changes in the network topology.

Reference: *Cisco – HSRP Background and Operations.*
http://www.cisco.com/warp/public/619/hsrpguide1.html

Reference: *HSRP, Hot Standby Router Protocol.*
http://www.networksorcery.com/enp/protocol/hsrp.htm

HSRP Operation.

Hot Standby Router Protocol (HSRP) provides protection against fail over of IP traffic on the network to hosts that do not support dynamic router discovery. Using HSRP, a group of routers present an illusion of a single virtual router to the hosts that operate on the network. These group/groups of routers are known as HSRP group. Each HSRP group has a MAC (Media Access Control) address and an IP address.

A single router selected from the group, is primarily responsible for forwarding the packets that have been sent by the hosts to the virtual router. This router is known as the active router. There is also a standby router, which is kept as a backup for the active router. If the active router fails for some reason, the standby router assumes the role of the active router and begins to forward the packets. Another router from the HSRP group becomes the standby router.

Reference: *HSRP, Hot Standby Router Protocol. RFC - 228.*
http://www.faqs.org/rfcs/rfc2281.html

b) To detect or solve network problems it can sometimes become imperative to login to the network from a remote location, gather data/information about the problem and make appropriate configurations to the network to solve the problem. Remote access to systems is available through the Telnet protocol.

Multiple sessions can be used to reach the device that needs to be configured/modified. It's important to understand that the changes/modifications that

are being introduced take effect immediately, without having to boot/partially reboot the system or take users off the system.

c) Support for mobility is quite important when it comes to making changes on the network (e.g. adding / moving hosts on the network). From an organizational perspective, it costs a lot to move the users around the network. Tools such as ***Dynamic Host Configuration Protocol (DHCP)*** relay support in Layer 3 switches, and allows the network administrators to centralize the assignment of IP addresses in an organization's network. The Dynamic Host Configuration Working Group of the Internet Engineering Task Force created DHCP. When an organization sets up a user on the network (i.e. gives internet access), an IP address needs to be assigned to the machine.

Without the Dynamic Host Configuration Protocol (DHCP), the IP address has to be entered manually in each computer. If the computer moves to another location, the IP address has to be given again. With DHCP, a device can have a different IP address every time it connects to the network. Dynamic IP addressing simplifies the job of network administrator because it's the software that keeps track of the IP addresses rather than the network administrator. Now a computer can be added to the network without the trouble of manually assigning an IP address to it.

Reference: *Dynamic Host Configuration Protocol (DHCP).*
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213894,00.html
Reference: *DHCP.*
http://www.webopedia.com/TERM/D/DHCP.html
Reference: *Dynamic Host Configuration Protocol (DHCP) FAQ.*
http://www.dhcp-handbook.com/dhcp_faq.html#widxx

d) An important aspect in network management is to remotely troubleshoot the problems that might plague the network. The layer 3 switches come with an extended suite of online network debugging capability that allows network administrators to remotely troubleshoot the problems. Without such kind of debugging functionality the network administrators would have to deploy network analyzers at different points in the network to monitor the network performance.

Protocols such as ***Simple Network Management Protocol (SNMP)*** and ***File Transfer Protocol (FTP)*** are especially important. SNMP is used to collect information about errors, and is designed to facilitate the exchange of this information amongst the network devices. Information on throughput, network error rate can be useful to the network administrators in managing the network, and resolving problems on the network.

FTP is used for sending software / configuration files across the network, downloading programs and other files to the computer from other servers, and thereby making administration of the network much easier.

Reference: *Simple Network Management Protocol (SNMP).*
http://www.cisco.com/warp/public/535/3.html
Reference: *Simple Network Management Protocol (SNMP).*
http://webopedia.internet.com/TERM/S/SNMP.html
Reference: *File Transfer Protocol (FTP).*
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213976,00.html

There are other network debugging tools such as the syslog feature that has been integrated into the Cisco IOS software. This feature aids network managers in collecting error information and network debug information that will be useful in analyzing the network problems. This capability is useful only if the information

received, is time stamped and the system computer clocks are synchronized in all the Layer 3 switches.

The ***Network Time Protocol (NTP)*** component of the Cisco IOS software is used to perform time synchronization between the Layer 3 switches and the switches in the wiring closet as well. The Network Time Protocol is a time synchronization system for the computer clocks throughout the network. NTP uses ***Coordinated Universal Time*** (Formerly and still widely called Greenwich Mean Time) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond. NTP has the following characteristics:

- Fully automatic, keeps continuous synchronization.
- Suitable to synchronize the entire computer network.
- Synchronization accuracy to 1 millisecond

Reference: *Network Time Protocol (NTP).*
http://toi.iriti.cnr.it/uk/ntp.html
Reference: *NTP.*
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci283988,00.html
Reference: *Coordinated Universal Time.*
http://whatis.techtarget.com/definition/0,,sid9_gci213612,00.html

e) All the network devices that form the core of the network are considered as a strategic asset of the company, and thereby need to be safeguarded against the possibility of unauthorized users gaining access to the system and causing disruption of network services. A couple of security mechanisms that are used in routers are as follows: -

. **Access Control Lists** – Its a table that tells the computer operating system which access rights each user has to a particular system, application or a network. Each ACL has numerous access control entries (ACEs) consisting of the name of a

user, group of users and applications that are to be denied or granted access through the port where the ACL is applied. The Network Administrator creates the ACL for hosts/host groups that operate on he network. It can also be used to restrict traffic on the network. Access Lists are provided on the nodes with explicit instruction to allow or deny traffic originating from specific protocol type or IP address. Creating Access Control Lists is a good way of restricting unwanted traffic on the network.

***Reference**: Access control list (ACL).*
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213757,00.html

. **Host Access Protection** – Security features needed for host protection include mechanisms such as encrypted passwords and configuration files, authentication of user logins and record login attempts. Such an operational infrastructure needs to remain intact when migrating to Layer 3 switches.

What's the tradeoff involved in using Layer 3 Switches as a forwarding mechanism?

1. Performance issues related with Routers and Layer 2 Switches.
2. Can Layer 3 Switching increase Bandwidth?

Performance issues related with routers and layer 2 switches.

Until recently, routers were the only option available amongst the network administrators to divide the workstations into separate broadcast domains or different LAN's. A broadcast domain is defined as a network in which a broadcast frame can travel from end-to-end. The perimeter of a broadcast domain is defined by the physical boundaries of the network or by a router. Routers don't forward broadcasts. Hence to communicate from one network to the other network, routers are required. Every port on

the router represents a separate network. This means that in an IP/IPX environment, each port has a different logical network address.

It is also important to know that within a single broadcast domain there can be several collision domains, created with hubs and switches. Routers then use different algorithms to calculate the most efficient path to forward the packets towards the destination station. Routers forward packets based on network address. This allows routers, the ability to filter packets, and help secure the network from unwanted packets. However, this has an impact on router performance and makes them slower as compared to Layer 2 switches.

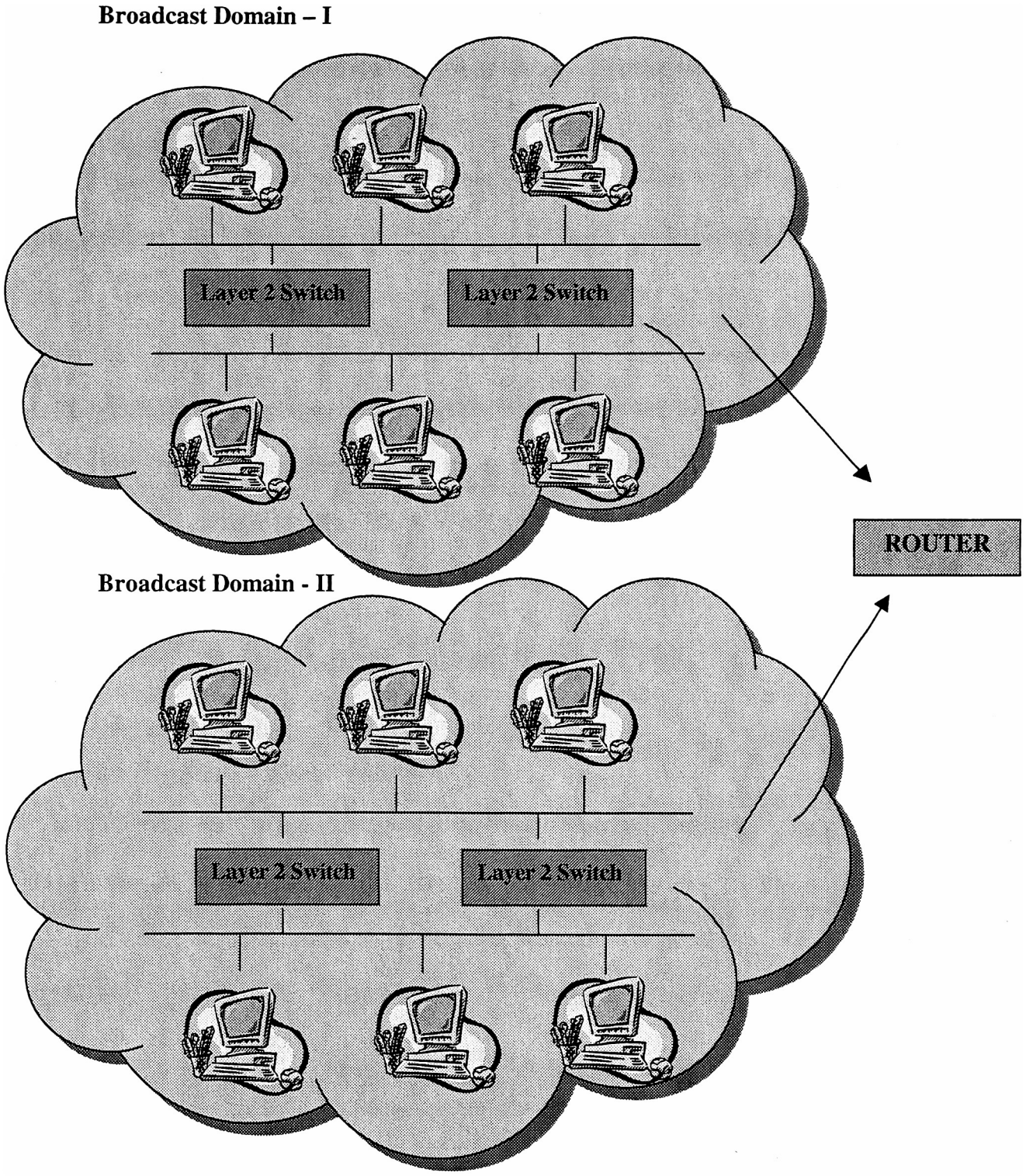
Layer 2 switches operate on the base of MAC addresses. They operate at a higher speed as compared to routers, have higher throughput and lower latency, and are cheaper as compared to the routers. This makes the switches faster and efficient to operate. "*One strategy amongst the Network engineers in the early years was to create networks that were less dependent on routers*". The Network engineers were encouraged to place more workstations in a single Layer 3 network. The idea behind such a strategy was to avoid routing as far as possible and implement a flat network. With more switches in the network, the number of workstations can be increased in a single broadcast domain.

Hardware was no longer a criteria to determine the number of workstations that would be a part of the broadcast domain. Through VLAN (Virtual LAN) technology, a software-defined network can be enabled whose boundaries are independent of the physical media. VLAN defines the boundaries of a broadcast domain through the software and users/organizations needs. Inside a VLAN, the transmission takes place at wire-speed and with a lower latency factor as compared to a router. VLAN supports

network segmentation the way network administrators want, because they can actually pick and choose the ports that will belong to a VLAN. The network administrators can have several ports of the same switch or ports from multiple switches as part of a single VLAN. Multiple switches in a single VLAN allow the administrators to overcome distances that were previously forced upon by the Ethernet.

Through the use of Layer 2 switches, the administrators thought that routers could be avoided and more workstations could be added on to the network. The idea behind such a strategy was to make the size of the intranets smaller, by having more workstations per VLAN, and each workstation could potentially be its own collision domain. The strategy sounds good – perhaps the answer lies in the fact to have networks without routers. After all routers are more expensive and slower as compared to layer 2 switches. This argument has huge ***FLAWS***. We cannot do without routers.

Although VLAN's may seem to provide the solution by extending the layer 2 broadcast domains, (to avoid crossing the router) this isn't the perfect solution. Remember, a broadcast domain is confined to that VLAN only. There needs to be some sort of routing mechanism for members of different VLAN's to communicate with each other. Each VLAN has a separate and a unique network address. To communicate between two different networks, routers are required. Ordinary broadcast packets cannot cross the boundaries of the broadcast domain or VLAN.



Reference: *IP Passport (Accelar) - When to use switches and when to use routers.*
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

Through the use of layer 2 switches, problems within the intranet can be resolved. Data transfer would be done at wire speeds. With the growth/popularity of

Internet, the traffic pattern has had an enormous change. Earlier the traffic model used to be "80/20", i.e. 80% of the traffic used to be within the intranet and only 20% would be routed.

But now days, it's the other way round. Almost 80% of the traffic is routed and only 20% remains within the network. Having more layer 2 switches in the internetwork and consequently a large VLAN complicates issues for the presently overburdened routers. So even after making VLAN's in the network, we haven't saved anything. We have just managed to tax our presently over burdened routers, and cause more traffic jams in the network. Broadcast and multicasts along with slow convergence from spanning tree can cause lot of problems in the network. As a result, the layer 2 switches are not in a position to replace the traditional routers/layer 3 switches.

***Reference**: Switch Vs Router.*
http://www1.ietf.org/mail-archive/ietf/Current/msg11453.html

Can layer 3 switches increase bandwidth?

Routers were traditionally used to improve network performance in places where bandwidth was limited. They would prioritize traffic around congested links in order to give preference to mission critical applications. Routers have also been used to isolate broadcast traffic to certain network segments, in order to preserve bandwidth on the network.

Although the layer 2 switches achieve wire speed performance in the VLAN, they cause bottlenecks onto router performance that operate between the VLAN's. Secondly, layer 2 switches don't utilize the full bandwidth potential. Layer 2 switches use Spanning tree algorithm to forward packets to the correct destination station. In a typical Spanning Tree network only the root bridge is allowed to use both of its ports to forward

the packets. Other switches in the network have just one port in the forwarding state. The other ports are in a standby mode. They start forwarding only if the port that was forwarding goes down. Layer 2 switches are limited to a single path between two end stations as specified in IEEE 802.1 Spanning Tree.

Implementing Spanning tree algorithm prevents formation of loops in a network. It does take care of the redundancy problem from the network, but prevents network traffic from load sharing across multiples paths through the network. In a way it's not able to fully utilize the bandwidth available. Performance issues might be resolved using layer 2 switches, but the bandwidth issue still remains unresolved. Layer 3 switches on the other hand, *balance load* by allowing traffic to flow through multiple paths on the network.

For example purposes, consider a network with *three 100 Mbps* paths between two end stations. In a traditional Spanning Tree environment, only one path would be used as an active path, and the other two would be in a standby ("blocking") mode. Hence the bandwidth utilization in this scenario is just one third (1/3) of the total available bandwidth. Using Layer 3 switching in such an environment would provide 300 Mbps of aggregate throughput (100 Mbps per path). In this case, Layer 3 switching would deliver three times the amount of bandwidth utilization without making any change to the existing network topology.

Reference: *Can Layer 3 switching increase bandwidth?*
http://www.nwfusion.com/newsletters/lans/0601lan2.html

Why Layer 3 Switches?

Routing and switching are the essential ingredients of a sound and stable network design. A substantial cost and performance differential does exist between layer

2 switches and the routers. This cost and performance differential can be eliminated through the induction of layer 3 switches (routing switch) in the network. The layer 3 switches (routing switch) perform wire-speed layer 2 switching and IP routing at every port. Both the essential forwarding functions are included within one device, and work in tandem with each other.

The layer 3 switches use "***route once, switch many***" architecture. The basic idea behind such architecture is to make use of known packet formats, so that packet forwarding can be done at high speeds. When a layer 3 switch receives a packet, it conducts a check on the address. If the address doesn't exist in its table, the packet may have to be routed. The next time a packet comes with the same address, all traffic for that address will be switched at layer 2 speeds.

The Layer 3 Switch is able to achieve gigabit wire speed performance as it uses ***ASIC's (Application Specific Integrated Circuit).*** With such hardware in place, Layer 3 Switches can achieve forwarding rates that are much higher as compared to the forwarding operation within a router. With the use of ASIC's, the layer 3 switch doesn't have to depend on CPU for its processing needs. Layer 3 switches perform the forwarding task at the ASIC level, as compared to routers that need the CPU assistance to perform the forwarding operation.

There is a big performance difference in introducing the forwarding operation at the ASIC level as compared to the CPU level. CPU happens to be a shared resource. There is a direct relationship between the CPU performance and the processes that run on it. The more processes that run on the CPU, the more time it takes for the CPU to execute them. Layer 3 switches do have the CPU modules, but they aren't involved in the

forwarding operation. Layer 3 switches, by using ASIC technology are able support switching and routing functionality on any port at full wire speeds.

Reference: *Layer 3 switching – (ASIC) Chip-Based Functionality.*
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

Benefits of using layer 3 switches.

- Provides integrated layer 2 and layer 3 processing. With such a technology in hand, the network administrators can deploy both the functionalities in one device throughout the network.
- Conventional router/LAN based architectures are being replaced with architectures based on layer 3 switching. Layer 3 switches forward packets at wire speed performance, and cost much less as compared to routers.
- Layer 3 switches can handle large amounts of traffic from multiple VLAN's at gigabit Ethernet speeds. They are pushing the routers into the WAN environment from the traditional LAN environment.
- Layer 3 switching increases bandwidth utilization in the network. Unlike layer 2 switches which don't use all ports for forwarding *(Spanning Tree Algorithm allows layer 2 switches to use just one port for forwarding traffic. This is done to prevent loops in the network.)* , layer 3 switches balance traffic load by using all ports.
- Offers lower latency.

Reference: *Benefits of Layer 3 switching.*
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

Standard based Layer 3 architectures – MPOA & MPLS.

A Layer 2 Switch does deliver performance within a LAN, but does not address the issue of performance bottlenecks between LAN's. The Layer 3 switching architectures are addressing these performance challenges. There are a number of vendor specific Layer 3 switching schemes, such as Cisco's tag switching, Nortel's Virtual Network Switching, IBM's Aggregate route based IP Switching etc. All of these architectures operate with the outside world using protocols such as OSPF and RIP. Two standard based Layer 3 architectures have been defined.

1) Multi-Protocol Over ATM (MPOA)

2) Multi-Protocol Label Switching (MPLS)

Multi-Protocol Over ATM (MPOA).

MPOA enables fast routing of packets through the network by replacing multi-hop routing with point-to-point routing. This is done by establishing a direct Virtual Channel Connection (VCC) between ingress device and an egress device. An ingress device or a host is defined, as a point through which there is an inflow of packets into the MPOA system. An egress device or a host is defined, as a point through which there is an outflow of packets from the MPOA system.

Benefits of Multi-Protocol over ATM (MPOA).

a) Eliminates the need for multiple router hops between the source and the destination station, by establishing a Virtual Channel Connection (VCC) between the hosts. The IP/other protocol packets then take the path established by the VCC.

b) Reduces the workload of the router by making less router hops for a packet to reach its destination.

Reference: *Multi-Protocol over ATM (MPOA) Overview.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/switch_c/xcprt7/xcmpoa.htm

MPOA Operation.

In a normal intersubnet routing operation, packets are forwarded to the destination station, hop-by-hop using the intermediate routers. MPOA operation can increase the network effectiveness by identifying and establishing a direct VCC connection between the ingress and egress edge devices, forwarding the Layer 3 packets over this connection, and thereby eliminating the use of intermediate routers. In this way, MPOA provides cut-through switching and reduces cumulative latency by minimizing the number of points where packet processing must be performed.

Reference: *Article on Layer 3 Switching- The enabler of IP-optimized Networking.*
http://www.nortelnetworks.com/solutions/financial/collateral/sept98_l3_switch_v1.pdf

Multiprotocol Label Switching (MPLS).

MPLS is a switching technology that improves network performance through efficient designation, forwarding and switching of traffic flow on the network. MPLS operation on the network involves setting up a specific path through the network that'll be taken by a given sequence of packets, identified by a label that's put in each packet. This aspect improves network performance and speed as the router need not lookup in its table of known addresses for the next node to forward the packet to.

Why use Label Switching?

The reasons to adopt label switching as a forwarding mechanism are quite important in improving the network performance. The following reasons have generated a keen interest in the industry: -

1. *Speed and Delay.*
2. *Jitter.*
3. *Scalability.*

Speed and Delay.

Traditional software based forwarding is too slow to handle large amounts of traffic on the Internet. Traffic load on the router is more than what it can handle. The result is lost traffic, lost sessions and overall poor performance in an IP based network.

Label switching, as compared to traditional IP based forwarding, is quite efficient in resolving the *Speed and Delay* problem. During a typical MPLS operation a label is placed in the packet's header. Forwarding decisions during MPLS are made on the base of label look-up in the forwarding table, as compared to an IP address lookup in case of a typical router operation.

Unlike forwarding on base of IP addresses, the labels that are used to forward the packets don't have to be unique. The same label can be used to forward more than one packet, and hence the time taken for a label look-up in the forwarding table is much less as compared to an IP address look-up. This aspect reduces latency and traffic queues at network interfaces. This reduction in traffic overhead is the *essence* of label switching technology.

Jitter.

During transmission of packets across the networks there is another component that's attached to the delay factor. It's the variability of delay associated with network traffic. The variability of delay in packet transmission arises as the packet traverses through several nodes before it reaches its final destination. This delay might not be the same at every node as every node on the network might have a different traffic pattern associated with it. Some nodes get more traffic than the others, and hence the term variable delay comes into existence.

As a packet traverses through numerous nodes on the network before it reaches its final destination, it experiences both delay and variable delay. This delay is directly proportional to the time it takes to conduct a table look-up for the address and the number of packets that are there in the buffer queue, waiting to be processed. The end result is jitter at the receiving station, caused by an accumulation of delays between the source and the destination station.

The situation becomes worse in case of digitized voice packets, because delay often translates into uneven speech play to the person listening to the speech. It may also result in the person having to wait for a couple of seconds to receive the last part of the sentence as the packets make their way through the network to reach the destination station. Label switching turns out to be more effective, as user's traffic can be sent through the network much faster with less jitter than the traditional IP based routing operation.

Scalability.

Speed is definitely an important component of Label switching. Processing user traffic on the network is also essential. But speed, and processing user traffic are not the

only things that label switching provides. Label switching also provides *Scalability*. The term scalability refers to the ability/inability of the system to accommodate growing number of users on the network. Thousands of users and the supporting interfaces (such as routers and switches) are being added on to the network everyday. The task of the routers is getting tough day by day as they have to keep a track of the changes that take place in the network topology as more users are added onto the network. This directly translates to more network addresses being added to the routers forwarding table, and hence the look-up time increases.

Label switching offers the solution to keep a track of all the users in a much more effective and concise manner. It allows large number of IP addresses to be associated with one or few labels. This approach reduces the size of the look-up table, reduces latency and allows a layer 3 switch to support more users.

Reference: *MPLS and Label Switching Networks - Why use Label Switching.*
Black, Uyless D., MPLS and Label Switching Networks, Prentice Hall Series, 2001

MPLS performs the following functions.

a) Provides means to map IP addresses with labels used by different packet switching / forwarding technologies.
b) Works with different protocols such as IP, ATM and Frame Relay.
c) Enables network administrators to manage traffic more effectively on the network by diverting traffic around link/node failures, congested interfaces and other bottlenecks that plague the network.

MPLS Operation.

During the MPLS operation, the data transmission takes place on Label Switched Paths (LSP's). These LSP's are sequence of labels that are provided at each and

every node along the path from the source to the destination station. These labels are protocol specific identifiers and are distributed using protocols such as Label Distribution Protocol (LDP), Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). Each data packet during the data transmission carries the label with it from source to the destination station. High speed switching is achieved as the label is used in routing the packet, and thereby avoiding the need to analyze the address field in every packet.

Reference: *Multiprotocol Label Switching (MPLS).*
http://www.iec.org/online/tutorials/mpls/topic03.html?Next.x=41&Next.y=12
Reference: *Multiprotocol Label Switching (MPLS).*
http://www.webopedia.com/TERM/M/MPLS.html
Reference: *Multiprotocol Label Switching (MPLS).*
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214350,00.html
Reference: *Article on Layer 3 Switching- the enabler of IP-optimized Networking.*
http://www.nortelnetworks.com/solutions/financial/collateral/sept98_l3_switch_v1.pdf

Need for Layer 3 Switches.

When the networks initially emerged, there was the need to extend them further in terms of distance, and as a result repeaters came into existence. Now there was a desire to connect LAN's over WAN's (Wide Area Networks). This aspect gave rise to bridges. And when more and more networks had to be connected, routers came into the arena. Organizations were still striving for more speed on their network. More speed meant having switches in the network topology. The first switch that came out was the Layer 2 switch that operated on the base of MAC address. Traffic on the network increased a lot, which created the need for more and more speed. This meant progressing towards Layer 3 switches. A layer 3 switch supports high IP/IPX performance and routing protocols such as RIP, OSPF, IGRP, and EIGRP.

Reference: *Layer 3 Switching – Need for layer 3 switches.*
http://www.mouse.deamon.nl/ckp/lanwan/13switch.htm
Reference: *Layer 3 switching.*
http://www.cisco.com/warp/public/779/largeent/learn/technologies/L3_switching.html

Layer 3 Switch Vs the Traditional Router.

Characteristic	Layer 3 Switch	Traditional Router
Routes protocols: IP, IPX, Apple Talk.	Yes.	Yes.
Forwarding Architecture.	Hardware.	Software.
Price.	Low	High.
Forwarding Performance.	High.	Low.
WAN Support.	No.	Yes.

Reference: *Layer 3 switch Vs Traditional router.*
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

Layer 4 Switching.

Layer 4 switching takes place at the Transport layer of the OSI model. The Transport layer takes care of things like: -

- *Flow control of data across the network.*
- *Reliable and accurate delivery of data.*
- *Provides error checking to ensure error-free data delivery to the destination.*
- *Provides acknowledgement of successful transmissions and requests retransmission if packets don't arrive error-free.*
- *Determines the type of service to be provided to the session layer and to the users of the network. This type of service is determined once the connection has been established. The quality of service is accomplished as Layer 4 uses protocols such as TCP and UDP to forward the packets.*

Reference: *OSI Model Layers*
http://geocites.com/SiliconValley/Monitor/3131/ne/osimodel.html
Reference: *The Seven-Layer Model. – The Transport Layer*
http://www.rad.com/networks/1994/osi/transp.htm

Common Suite of TCP/IP Protocols related to the OSI model.

7	TELNET	FTP	SMTP	SNMP	DNS
6		File Transfer Protocol RFC-959	Simple Mail Transfer Protocol RFC-821	Simple Network Management Protocol RFC-1098	Domain Name System RFC-1034
5					
4	***TCP RFC-793***			***UDP RFC-768***	
3	ARP RFC-826	RARP RFC-903	ICMP RFC-792		BOOTP RFC-951
	IP				
2	802.1	802.2	802.3	802.4	802.5	802.12
1	802	802.2			

Reference: *The OSI Seven-Layer Model- Common suite of TCP/IP protocols*
http://www.netc.org/network_guide/c.html

The transport layer is responsible for end-to-end communication between the network source and the destination systems, and uses protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). At Layer 4, the switching decisions are made not only on the basis of MAC address or source and destination IP address but also on the basis of TCP/UDP application port number.

The TCP and UDP headers contain port numbers that help in identifying which application protocols (e.g. HTTP, SMTP, FTP etc.) are included within the packet. The switch uses this information to analyze and interpret the data that's contained within the packet. In particular, the port number enables a switch to identify the type of IP packet it has received and enables the switch to hand it off to the most appropriate server. This information is extremely useful in handling network traffic.

The combination of the TCP or UDP port number inserted in the packet along with the IP address is commonly referred to as a socket. Many well-known applications such as HTTP and FTP use designated ports.

Reference: *Layer 4 Switching.*
http://www.msic.com/ebusiness/convergence/layerswitch.shtml

The port numbers between 1 and 255 are known as 'well known ports'. This is precisely because they are the same in every host TCP/IP protocol stack implementation. Apart from these well-known port numbers, standard Unix services are assigned port numbers from 256 to 1024. Custom-developed applications are assigned port numbers above 1024. These port numbers are assigned by IANA.

Examples of well known port numbers.

Application Protocol	Port Number
FTP	20 & 21
TELNET	23
SMTP	25
HTTP	80
NNTP	119
SNMP	161 & 162

Reference: *Well known port numbers.*
http://www.freesoft.org/CIE/RFC/1700/4.htm

An intelligent aspect of Layer 4 switching is the ability to identify and analyze two important pieces of information, viz. port number and the packets IP address. With these two vital points of information in hand, the Layer 4 switch not only knows where the data needs to go, but also what application is going to use the data. This provides the network, the opportunity to differentiate between applications when making routing decisions. For e.g. traffic meant for important/mission-critical applications (i.e., SAP R/3, Peoplesoft, Baan, custom developed client/server application) can be assigned different forwarding rules as compared to HTTP based traffic, even if both kinds of traffic need to travel through the same switch or router interface. The ability to classify application specific traffic is extremely important and enables prioritization of traffic, based on how critical it is to the business. This is done as the switch is able to access the port number and the IP address of the packet, thereby giving priority to time sensitive/mission-critical applications.

Reference: *Layer 4 switching.*
http://www.comtest.com/tutorials/layer4.html

Layer 4 Switching: Hope or Hype?

The concept of Layer 4 Switching has been in existence for quite some time. When it was first introduced, people/companies were quite skeptical about the term "*Layer 4 Switching*". People connected with the Networking industry knew the order and the sense of the OSI reference model. Switching could be done at Layer 2 i.e. the Data Link Layer of the OSI model, because that was the place where you found the MAC address. Switching was simple out here. Just forward the frame based on the destination MAC address. Switching could also be done at Layer 3, i.e. the Network Layer of the OSI model, because that was the place where you found the IP (Newtwork) address – if protocols such as IP/IPX were being used.

The initial skepticism laid in the very fact that Layer 4, i.e. Transport Layer of the OSI model does not contain any addressing information. The primary question, therefore was, " *If Transport Layer does not contain any addressing information, how can it switch packets?* ". It is the Transport Layer of the OSI reference model, where information regarding application services or protocols that might be using the IP network, can be found. For instance one can come to know that it was TCP rather than UDP that was sending data to the IP layer, or that it was HTTP traffic instead of FTP traffic that was being sent through the network.

The answer to the question lays in the fact of looking at the network flow rather than just the movement of packets across the network, from source to the destination station. Switching at Layer 4 identifies a stream of packets by more than just its MAC or Network address. Additional information from Layer 4 is taken into account to form a

much larger picture, thereby creating an extremely precise and more expansive set of information for packets that move across the network. The packet stream, although still identified by its MAC and the Network address, is further refined by identifying the nature of the application within the packet. The Layer 4 switch not only knows where the data needs to go, but also what application is going to use the data. This provides the switch, the ability to differentiate between applications when making forwarding decisions.

With all this information in hand, *it becomes possible to identify the application flow*, rather than just the fact that packets were moving from source station A to destination station B. Through Layer 4 switching, it is possible to identify one flow from source station A to destination station B as HTTP traffic and another flow from source station A to destination station B as FTP traffic. As application flow awareness increases with Layer 4 Switching, it becomes possible to apply different rules to different streams of traffic as they move through the network. This becomes a necessity, as all traffic flows cannot be granted similar preferential treatment. Depending upon the critical importance of the application flow, rules can be set in place to give preferential treatment to one set of traffic over the other. For e.g. if both HTTP and FTP traffic is moving from station A to station B, HTTP traffic can be given *precedence* over the FTP traffic, even though the traffic is moving between the same source and the destination station. This is quite an important aspect as the networks carry different types of traffic. Networks of today are loaded with packetized voice/video streams along with other types of data. Identifying multimedia packets on a layer 4 basis can be used to ensure that they get a higher priority over other kinds of traffic on the network.

Reference: *Layer 4 Switching: Hype or Hope*
http://www.sterlingresearch.com/library/library/05_98layer4_switching.html

Packet filtering and Prioritization.

Examining Layer 4 information when making a forwarding decision is not a new concept. The ability to define routing based filters is a standard feature of software-based routers, and is used for the purposes of security. Routers are often used as network firewall. They filter packets and provide security features by either allowing or blocking network traffic from certain interfaces. These filters act as packet-filtering firewalls because the routers check the traffic based on source and destination IP addresses and the port numbers. These routers use layer 4 information solely for the purposes of security.

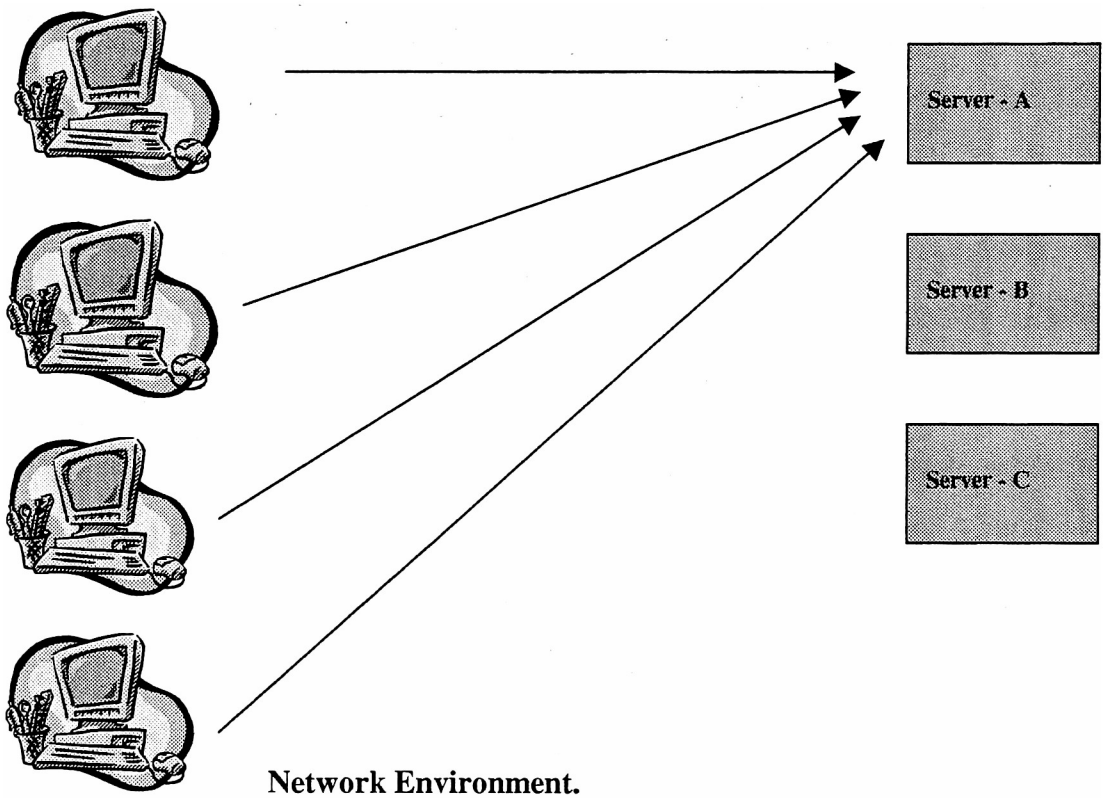
On the contrary, Layer 4 switching has got more to it than just the establishment of access lists as firewalls between various network segments. A layer 4 switch offers the same service, but implements it by means of hardware, thus offering much higher data throughput. By implementing Layer 4 switching in hardware (ASIC's, Application Specific Integrated Circuits), the switches can apply security filters at wire speeds. Layer 4 switching enables prioritization and switching of traffic based on the application type. As the Layer 4 switches can see both the port number and the packets IP address, it not only knows where the data needs to go, but also what application is going to use the data, and can therefore give priority to the data intended for mission critical applications

Reference: *Layer 4 Switching.*
http://www.comtest.com/tutorials/layer4.html
Reference: *Layer 4 Switching.*
http://www.tbg.com/Public/WhitePapers/L4_switching.html

Load Balancing.

Another service that can be made possible through the use of Layer 4 switching is load balancing. In a traditional network configuration, each server has a unique IP

address. A situation might occur when one server might be fully loaded with network traffic while the other servers might be sitting idle, simply because all the users are targeting their server request to the first available IP address. In such a situation, load balancing can be implemented to control the amount of traffic a particular server among a group of servers supporting the same application, receives.



Network Environment.

In the following diagram we see a typical situation that might occur if there is no system in place to properly direct the server requests. As depicted in the diagram, all the workstations are directing their requests to Server – A. As more and more workstations are added onto the network and they start directing their requests to Server – A, the server

would become loaded with their requests and this would certainly impact its processing capability.

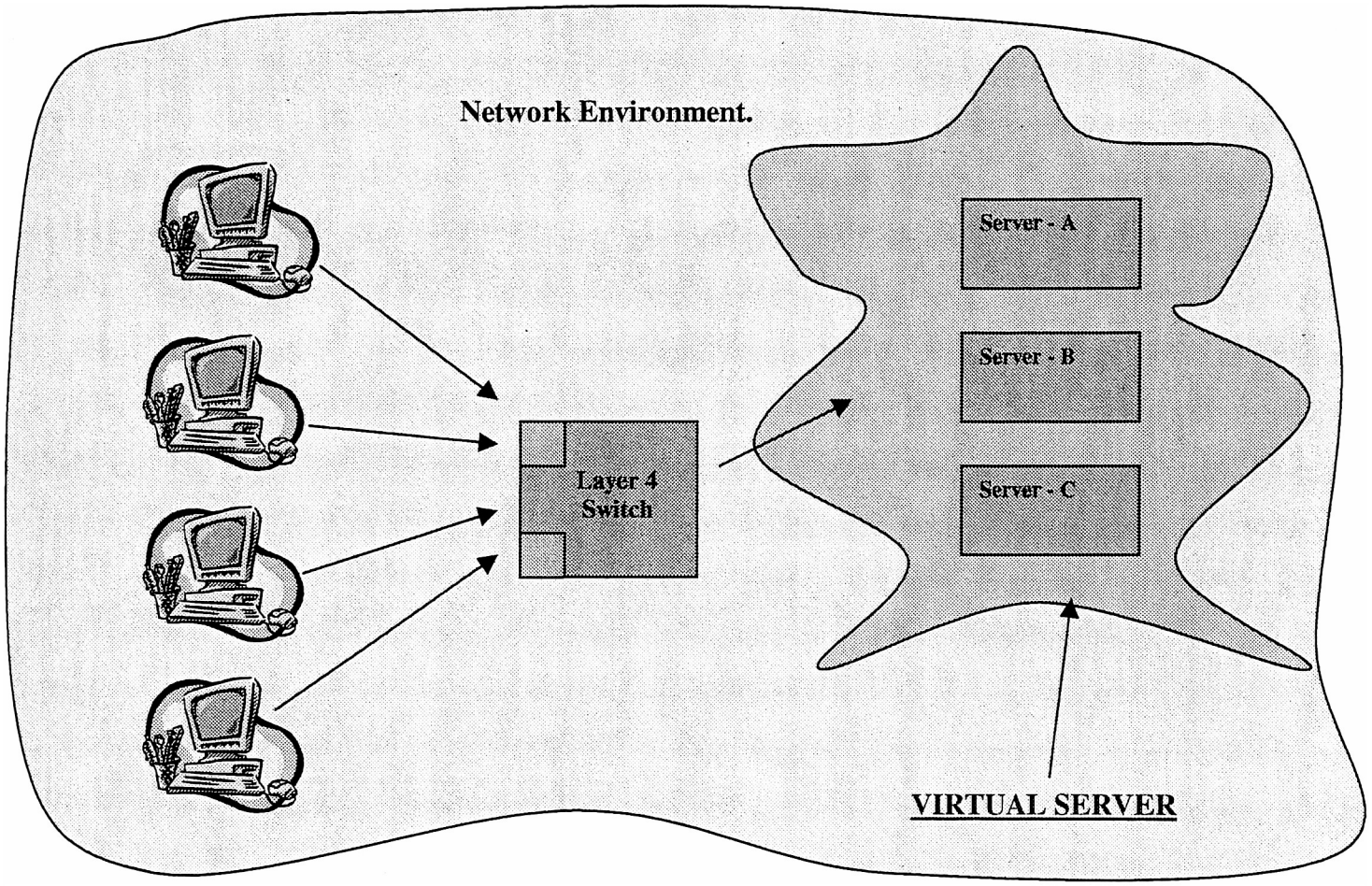
Switching at Layer 4 does reduce considerable amount of load off the server by doing a fine balancing act of sending traffic across a cluster of servers based upon the session information. This is achieved by grouping a set of physical servers that are being used as web servers into one *virtual or logical server*. The new virtual server, made up of these physical servers is assigned one IP address. Now, the traffic that is assigned to these servers is directed to the IP address of that particular virtual server. So whenever a client requests for an application, the request is directed to the IP address of that virtual server *(VIP)*. The switch resolves the issue by determining which server (from the group of servers that make up the virtual server) will handle the client's request. The data traffic can be balanced amongst the servers that form the virtual server on a number of factors. For instance, by keeping a track of the number of sessions each individual server (of the virtual server group) is supporting, data traffic can be forwarded to the server with the least number of sessions. The data traffic can also be distributed on a percentage basis. The faster servers can be assigned a higher percentage of overall data traffic as compared to the slower servers. Once the switch makes a forwarding decision for a particular server in the virtual server group, it reserves the session for that particular server. This way the switch balances the traffic load amongst the servers.

Implementing switching at layer 4, allows the organizations to prioritize traffic based on specific applications. This type of service is pretty important for providing different levels of service for the networks of today and tomorrow.

Reference: *Layer 4 switching.*
http://www.comtest.com/tutorials/layer4.html
Reference: *Layer 4 switching: The magic combination.*
http://www.nwfusion.com/newsletters/lans/0215lan1.html

Reference: *Layer 4 switching.*
http://www.idg.net/crd_switch_67600.html

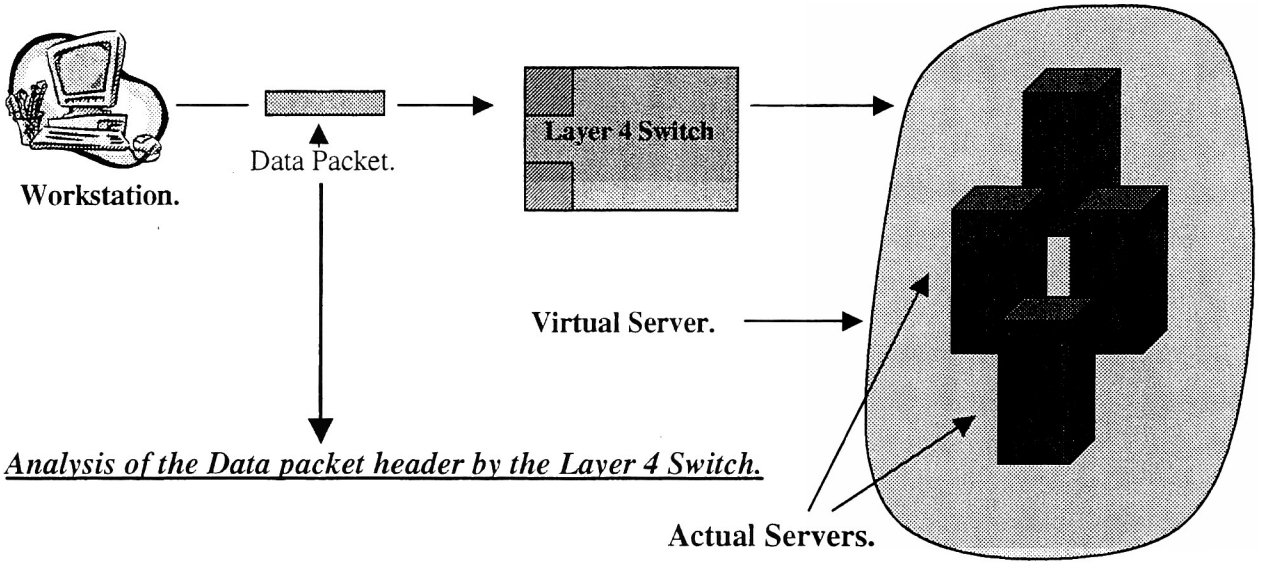
Scenario after the layer 4 switch has been placed in the Network.



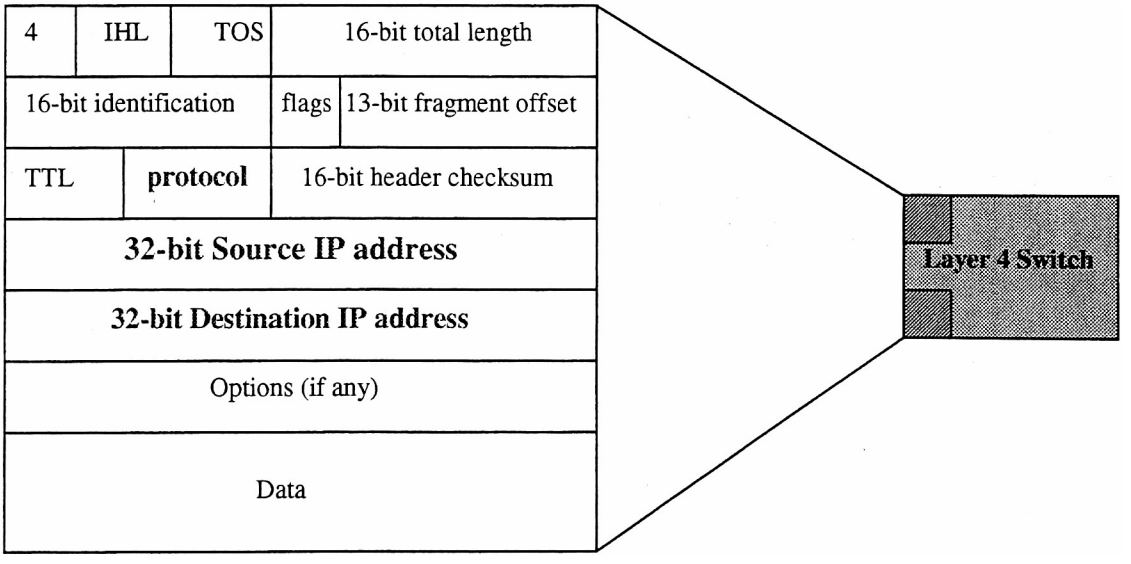
As it is evident from the above diagram, the layer 4 switch accepts the server requests from the workstations and passes it on to the virtual server.

Switching operation at Layer 4.

Layer 4 switching is about managing and switching application sessions, not just individual packets. The main reason for taking switching to layer 4 is to work around the problem of server congestion. Layer 4 switches can identify and process TCP/IP sessions at wire speeds.



Analysis of the Data packet header by the Layer 4 Switch.



Reference: *http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html*

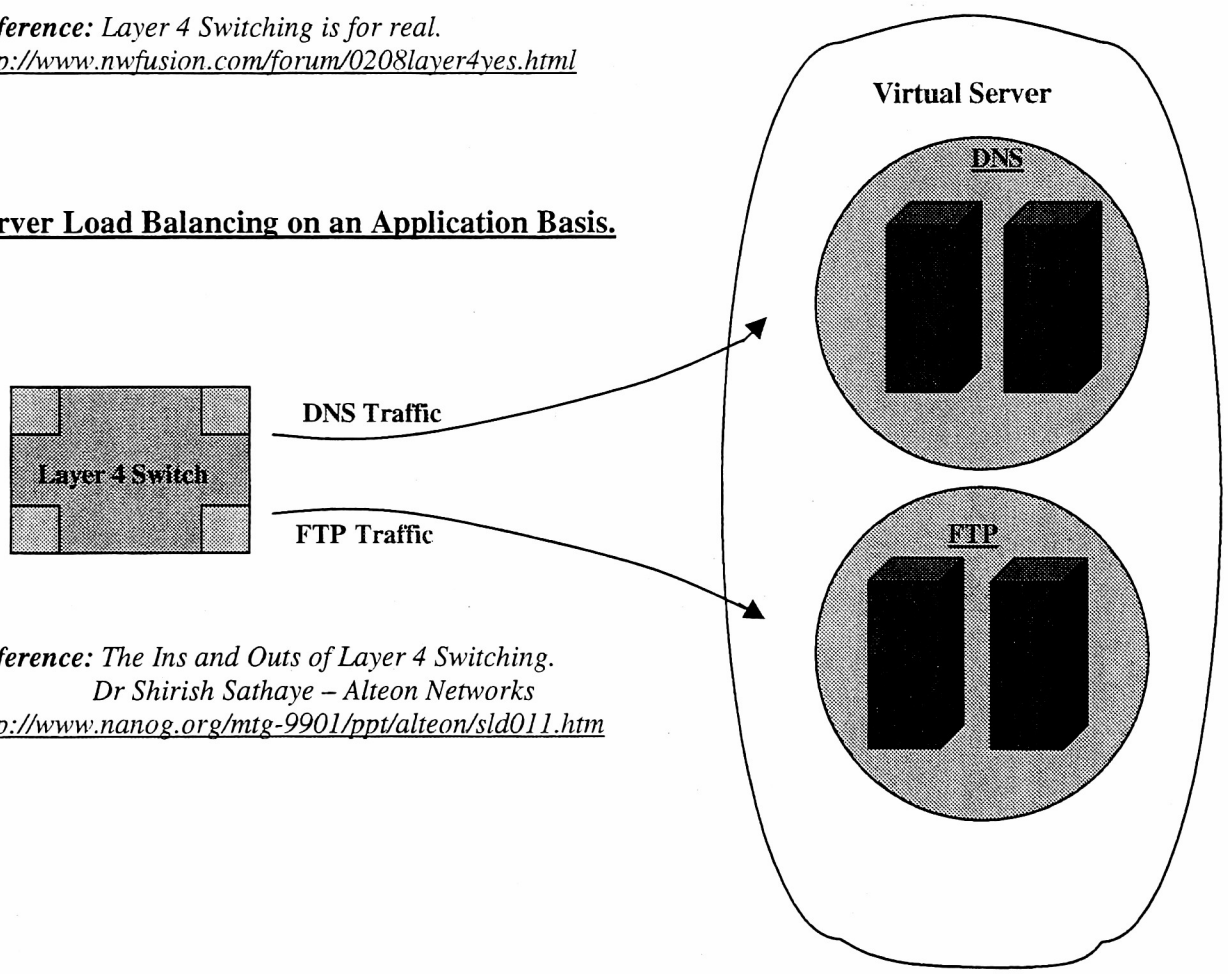
Layer 4 accepts the data packet intended for a particular server. In this process, the Layer 4 switch substitutes the IP address of the Virtual Server (VIP) in the destination

address field of the packet (The destination address field in the packet contains the actual IP address of the real/physical server). This move ensures that all packets within each TCP connection are forwarded to the same real server in a proper sequence.

Layer 4 switching technology transparently intercepts application traffic, by analyzing the TCP and UDP headers. These headers contain port numbers that help in identifying which application protocol (e.g. HTTP, SMTP, FTP etc.) is included within the packet. Layer 4 switches can also direct specific application requests to different servers.

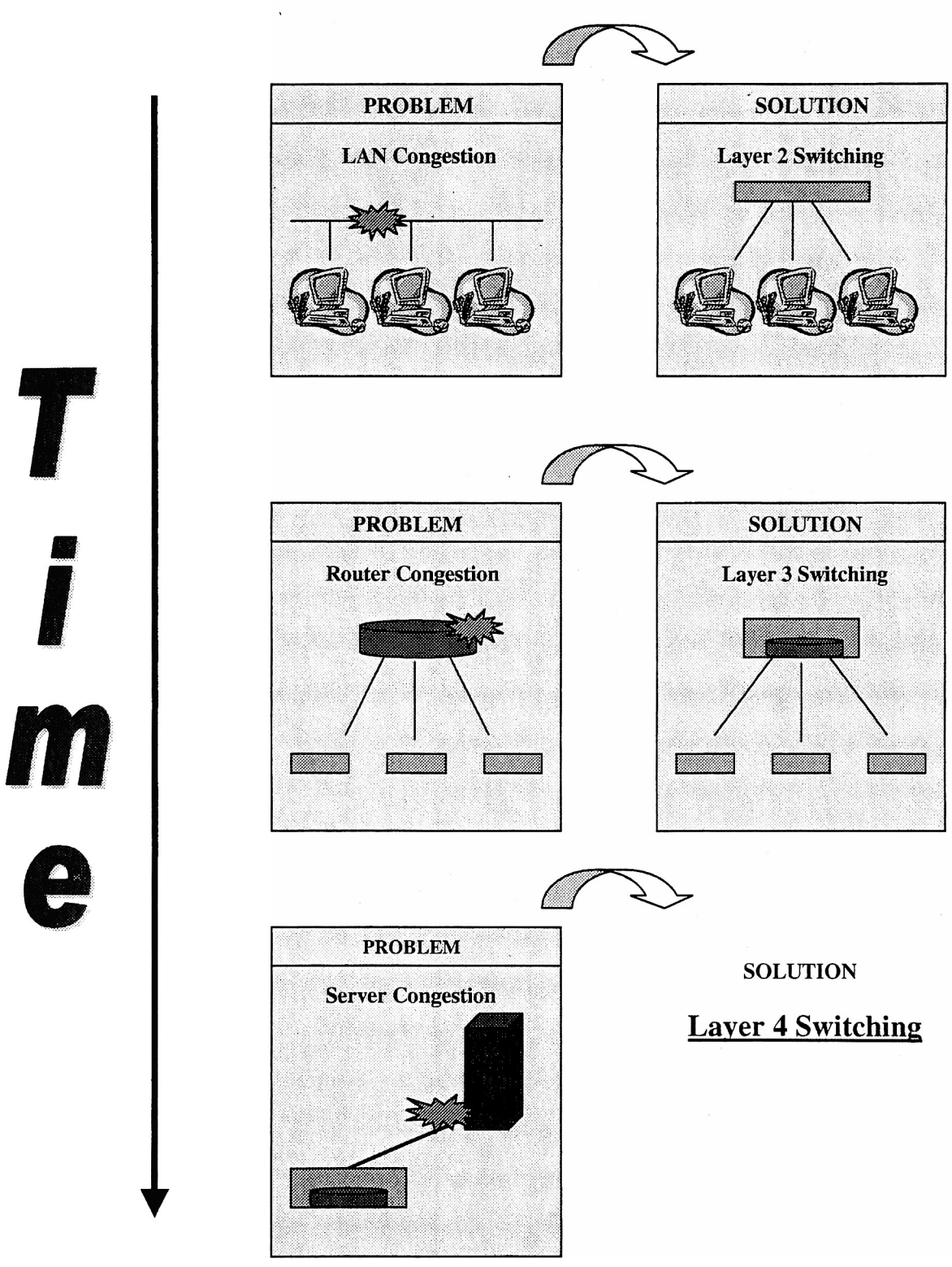
Reference: *Layer 4 Switching is for real.*
http://www.nwfusion.com/forum/0208layer4yes.html

Server Load Balancing on an Application Basis.



Reference: *The Ins and Outs of Layer 4 Switching.*
Dr Shirish Sathaye – Alteon Networks
http://www.nanog.org/mtg-9901/ppt/alteon/sld011.htm

Why is Layer 4 switching important?



Reference: *The Ins and Outs of Layer 4 Switching. Dr Shirish Sathaye – Alteon Networks*
http://www.nanog.org/mtg-9901/ppt/alteon/sld006.htm

Benefits of Application level control in Layer 4 Switching.

- *QoS (Quality of Service).*
- *Security.*
- *Accounting.*

Application –level QoS (Quality of Service).

The demand for Qos (Quality of Service) in the networks for today is constantly on the rise. The kind of traffic that travels across the network is extremely diverse and the quantum is increasing day by day. Rich data types, mixed media, video conferencing, real-time audio and video, Internet telephony, interactive transaction processing and mission critical applications, all create the need for tight control over latency and data throughput.

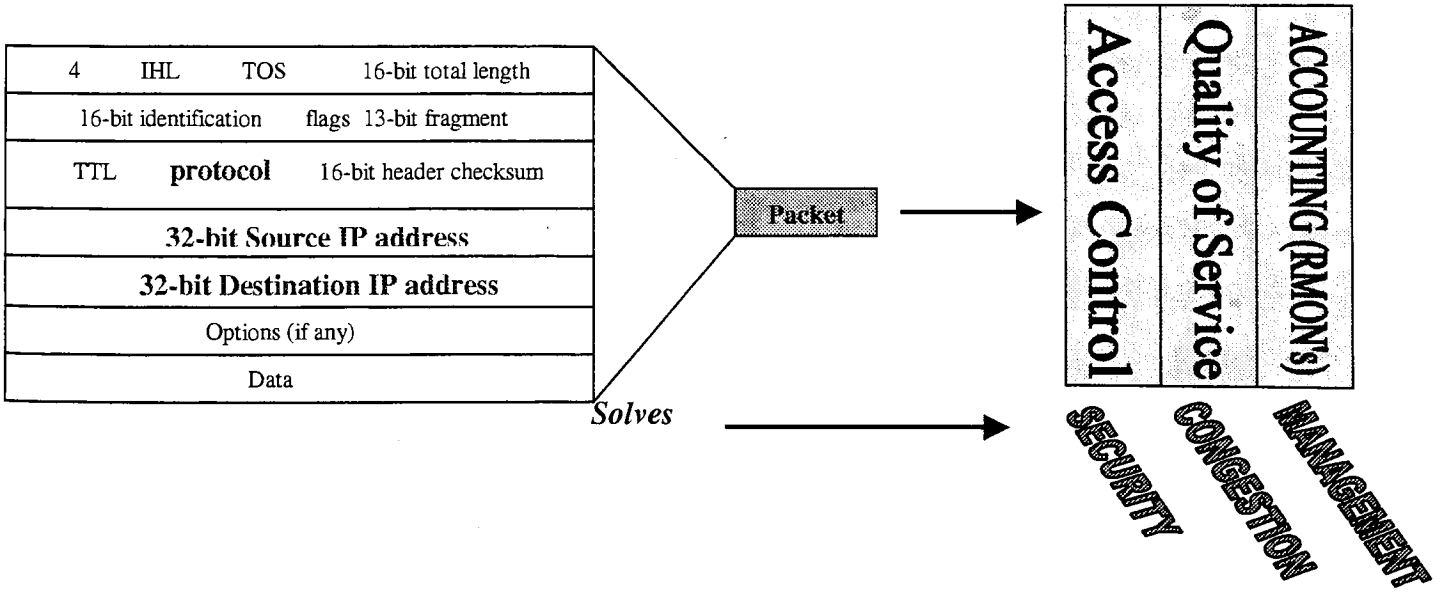
QoS refers to a set of mechanisms in place to meet the traffic flow needs by providing wire-speed bandwidth and low latency for all applications that run on the network. The need for QoS is felt the most when the switch ports are overloaded and the internal buffers are full. QoS prioritizes the flow of traffic by creating rules or policies that govern the flow of applications on the network. Layer 4 switching enables the QoS policies to be set on an application level basis. This gives the network managers a complete control over bandwidth utilization in the network. In layer 2/3 switching the QoS policies can prioritize traffic based solely on the source and the destination address. Taking switching to layer 4 means priorities can now be set on an individual host-to-host application conversation.

Reference: *Benefits of Application-Level Control. – QoS.*
http://www.enterasys.com/products/whitepapers/multilayer

Application – level Access Control.

Since the beginning, routers have used security filters and access control lists to provide a secure environment for the corporate networks and the databases. Access control till now consisted of software based processing, based upon Layer 2, Layer 3 and Layer 4 information in every packet and comparing that information with the list of allowed addresses or applications. The problem with software-based filter processing was that whenever the access control filters were enabled, the router performance went down. Now, when a packet comes to a router it compares the address/application in the packet with a list of allowed/blocked addresses/applications in its access list. As this list enlarges, the router takes more time to process the traffic. This is due to the increased number of instructions the central processing unit (CPU) is required to execute on every packet. This results in higher latency and a drop in router performance.

Application level control by a Layer 4 switch on a packet.



Reference: *Benefits of Application-Level Control. – QoS.*
http://www.enterasys.com/products/whitepapers/multilayer
Reference: *IP Packet Header.*
http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html

Layer 4 switching eliminates performance loss associated with security features when processing packets. A true Layer 4 switch delivers wire-speed performance when all the advanced features including security are activated. In Layer 4 switching, packets are processed in custom ASICs, and since the source and destination port information is tracked, application-level security can be coupled with wire-speed performance.

(Portions highlighted in the diagram above are analyzed by the layer 4 switch to conduct an application level control on the packet.)

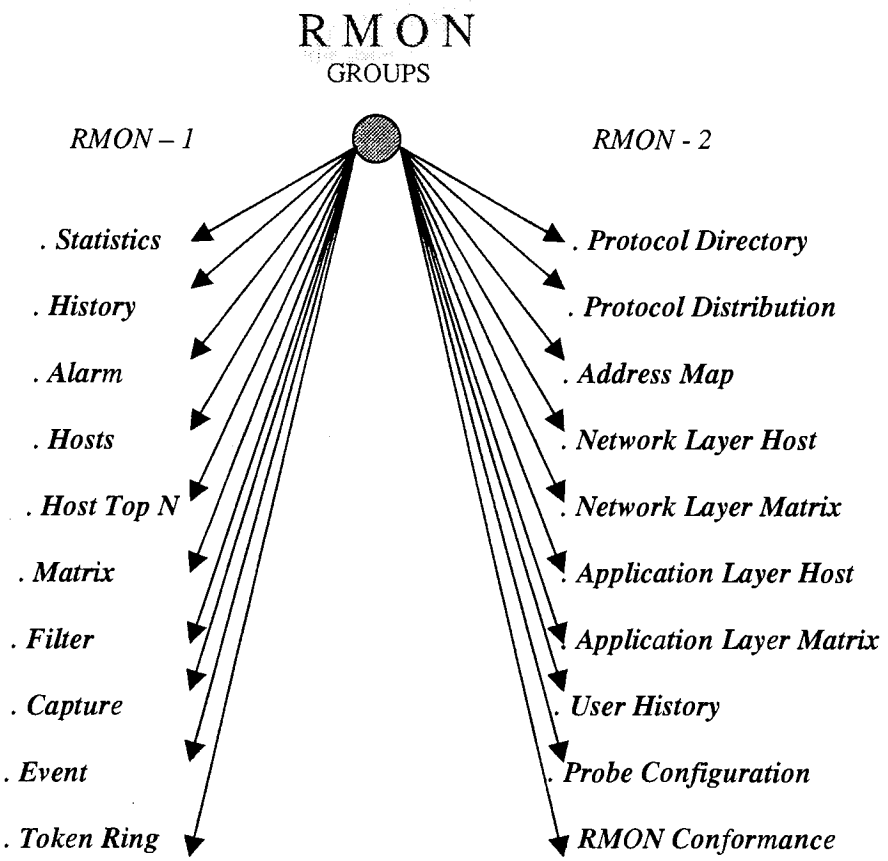
Application – level Accounting.

It's quite important for the network managers to monitor the performance of the network. If the performance cannot be measured, the network cannot be managed effectively. Layer 4 switches improve the performance of the network by not only monitoring the applications that travel across the network, but also keeping a track of the source/destination network addresses and source/destination port numbers for each flow. This enables the Layer 4 switch to collect information for each flow that passes through it.

Layer 4 switching supports *RMON* (Remote Monitoring) tools that collect application-level traffic statistics on a per port basis. RMON (Remote Monitoring) is a standard specification that allows various network monitors to exchange network-monitoring data. It also allows network administrators the freedom to choose specific network monitoring probes that corresponds to their particular networking needs. Traffic collection based upon Layer 4 application information (in addition to Layer 3 IP headers) provides network managers the tool to conduct enhanced troubleshooting of network problems and perform more-detailed accounting of network usage. RMON was defined

by the user community with the assistance of Internet Engineering Task Force (IETF). It became a draft standard in 1995 as *RFC-1757.*

Reference: *Benefits of Application-Level Control. – QoS.*
http://www.enterasys.com/products/whitepapers/multilayer
Reference: *RMON (Remote Monitoring)*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm



Reference: *RMON Groups.*
http://www.rmon.co.uk/html/rmon_groups.htm

RMON – 1.

1. Statistics: This is a LAN activity report card. The Network administrators can get information on traffic volume, traffic type, etc.

2. History: Sets of statistics are made to compare traffic behavior and trend information during specific intervals of time. Such information can be quite useful when making traffic management decisions on the network.
3. Alarm: Threshold values can be set and mechanisms to signal the RMON client can be put in place if the values go above or below the threshold levels.
4. Hosts: New hosts can be discovered by checking out the new Mac addresses on the network segments.
5. Host TopN: The RMON probe can sort the host information on a specified statistic. For example, the Network Administrator can find out the top 4/5 clients contributing to the maximum broadcast traffic.
6. Matrix: This utility traces traffic information between two stations. Information on traffic volume and associated errors involved in data transmission between the two stations can be saved for future reference.
7. Filter: The RMON probes can filter out specific information with a packet for further probes.
8. Capture: This group specifies the number of filtered packets that need to be saved.
9. Event: This group takes care of transmitting the SNMP TRAP signals to the remote client.
10. Token Ring: This group takes care of the token ring activities and uses the information for Token Ring management.

RMON – 2.

1. Protocol Directory: Provides a list of protocols that the probe supports. This is quite useful for the RMON – 2 applications as they can find out which protocols

the RMON – 2 probes can support. This assumes lot of significance as the applications and protocols come from different vendors.

2. Protocol Distribution: Provides traffic statistics for protocols such as IP/IPX, concerning their distribution and trend information in the network.
3. Address Map: Conducts IP to MAC address mapping for various probes, thereby making it easier for the Network administrator to decipher and interpret data.
4. Network-Layer Host: Shows traffic statistics to and from each discovered host on the segment. Used for improving the placement of network interfaces to reduce bandwidth and latency associated with data transfer.
5. Network-Layer Matrix: Traffic statistics between the newly discovered hosts.
6. Application-Layer Host: Traffic statistics from each host sorted on a protocol basis. Provides additional information on use of applications such as web, telnet, etc.
7. Application-Layer Matrix: Provides traffic statistics for pairs of hosts on a protocol basis.
8. User History: Focuses on RMON – 1-statistic group variables to collect user data.
9. Probe Configuration: Mechanism to set RMON probe parameters remotely.

Reference: RMON Probe Groups
http://www.rmon.co.uk/html/rmon_groups.htm

Benefits of Layer 4 switching.

- Application specific Prioritization of traffic. Mission critical applications get a higher priority as compared to other applications on the network.
- Wire-speed data transfer based on Layer 4 application information, even over multiple Gigabit Ethernet connections. Switching logic in layer 4 switches gets

implemented in the hardware, which makes the forwarding operation much faster as compared to the routers that implement the switching logic at the CPU level.

- QoS (Quality of service) based on applications.
- Enhanced manageability of network traffic. Layer 4 switches not only know where the traffic is intended for, but also what application is contained within the packet.
- Effective load balancing on traffic basis. Traffic gets re-directed to a virtual server.

Reference: *Examining Layer 4 Information.*
http://www.tbg.com/Public/WhitePapers/L4_switching.html

Layer 5 Switching.

Layer 5 of the OSI reference model – The Session Layer.

- *Establishes and maintains sessions across the network.*
- *Provides synchronization services by establishing checkpoints in the data flow. If the session fails for some reason, only the data after the most recent checkpoint is transmitted.*
- *Manages dialogue control. Once the session has been established, traffic can be allowed in both the directions at the same time, or in one direction at a time. If the traffic control is set to be unidirectional, the session layer can keep a track of whose turn is it?*

Reference: *OSI seven layer model.*
http://www.geocities.com/SiliconValley/Monitor/3131/ne/osimodel.html
Reference: *The Session layer.*
http://www.rad.com/networks/1994/osi/session.htm

Why Layer 5 switching?

With the advent of Layer 4 switches in the networking environment, QoS could be delivered within the network, because the layer 4 switches could differentiate between the applications that were running across the network, by looking beyond the network layer. Layer 4 switches glean into the TCP and UDP header information, which helps in identifying the application protocol (e.g. HTTP, SMTP, FTP etc.) that is included within the packet. This switch uses this information to analyze and interpret the data that's contained within the packet. These capabilities are often referred to as Layer 4 filtering and forwarding. With this information in hand, the Layer 4 switch not only knows where the data needs to go, but also what application is going to use the data. This provides the network administrator, the opportunity to differentiate/prioritize between applications when making forwarding decisions. The point of concern out here is that the Layer 4

switches cannot differentiate between different types of web traffic / web applications. The TCP port for Web traffic (HTTP traffic) is ***port 80***. All web applications use the same port number. The layer 4 switch does not recognize the custom web applications made by an organization. The inability of layer 4 switch to differentiate between different types of web traffic / web applications, creates the need for switching to go to layer 5, i.e. the session layer of the OSI reference model.

Objective of Layer 5 switching / Session layer switching.

The objective of taking the switching function to layer 5 is to create a perfect blend between the functionalities of layer 4 proxies and the data handling capabilities of the switch into one system. They need to work in perfect co-ordination with each other.

***Reference**: Layer 5 / Session layer switching.*
http://www.cc.gatech.edu/~wooylee/Layer-5switch.pdf

Operation of a layer 5 switch.

When taking switching to layer 5 (session layer) of the OSI reference model, the switches are able to gather an idea about the web content that is being requested by the client. This is done through URL Parsing. URL (Uniform Resource Locator) is basically a reference or an address to a resource on the Internet. In simple terms it can be considered as a name or a file on the network. URL's have two major components that are separated by a colon (:). For example, in *"http://www.hotmail.com"*, **http** stands for the protocol identifier and **//www.hotmail.com** happens to be the resource name (content that's being requested by the client). The protocol identifier refers to the name of the protocol being used. The protocol in the above example is HTTP (Hyper Text Transfer Protocol, used to serve hypertext documents) that'll be used to retrieve the content.

URL parsing involves the following tasks: -

- The load balancer looks into the URL,
- Gets the information on what the URL says, (type of content being requested, i.e. secured/unsecured content and cacheable/non-cacheable content.)
- Analyses which request needs to go to the server, (in other words, requests that can be served through proxy caches need not be sent to the original server hosting the content. It would be a complete waste of bandwidth if all requests were sent to the web servers hosting the content.)
- Binds the session to the best available server in the designated group that is hosting the content.

Reference: *Analyzing the content - URL Parsing*
http://www.f5networks.com/solutions/whitepapers/http.pdf

The number of users on the Internet is growing day by day, and as a result more and more content/applications are being requested off the Internet. Such a scenario creates bandwidth and latency problems, as web servers get an increasing number of requests from existing and new clients. A direct consequence of such bandwidth/latency problems would result in increased delays experienced by clients in retrieving business critical applications. Much of the material from the Internet is retrieved quite often. The web servers have to cater to the same requests time and over again. This leads to unnecessary bandwidth utilization from the repeated content requests.

Through the use of Content Smart Cache Switching, (*Web Caching* - a concept being applied for the layer 5 switches) bandwidth/latency problems associated with sending the same requests to the original server hosting the content can be resolved.

Web Caching.

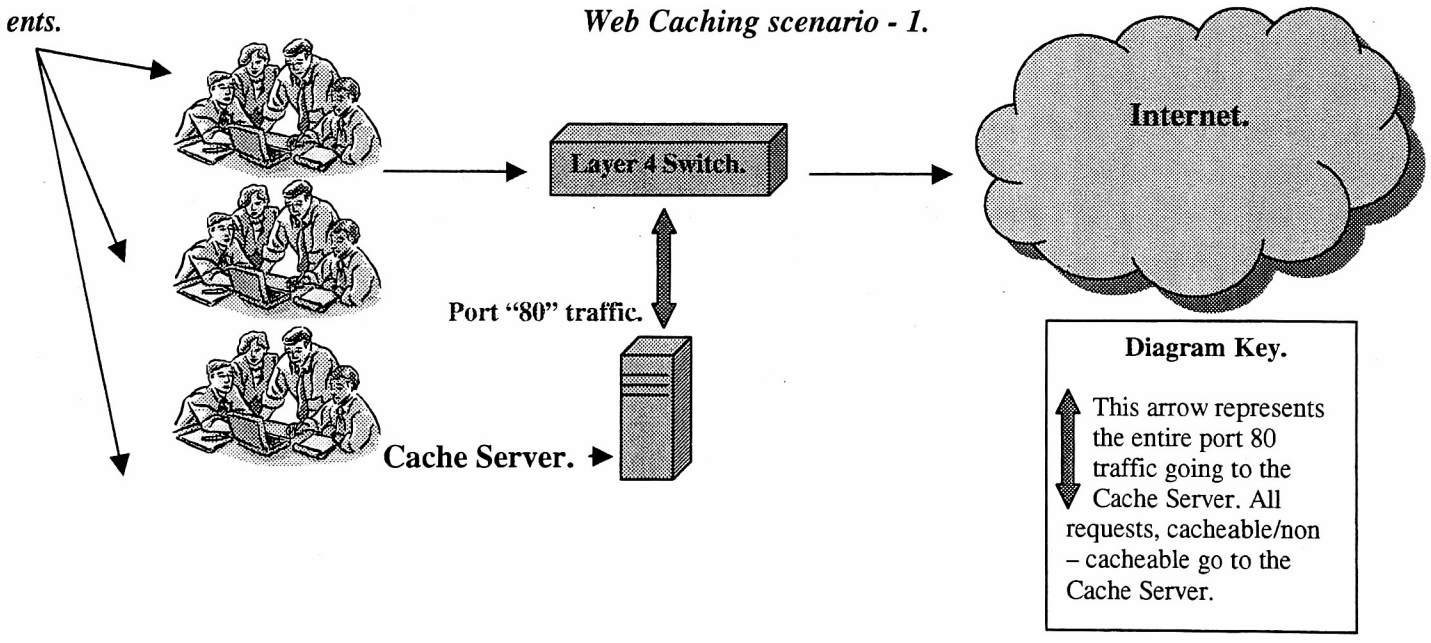
Web Caching as the name suggests, is a technology in place to store the client's request for material off the World Wide Web. The results of such web requests can be stored near the client's side, so that such kinds of requests don't have to traverse the same pipe lane time and again. The deployment of such kind of technology would largely be dependent on the goals and objectives of the company and their competitors. Web caching is enjoying a tremendous success especially at the international level, where bandwidth is expensive. Its importance and need is also beginning to make a presence at the US domestic front, where users network access needs are transforming from the traditional dial-up mode to broadband access to the web via cable modems and xDSL technology. Faster access to content needs faster processing mechanisms in place.

Web Caching / Cache Switching is a proactive method of storing specific content requests closer to the clients, intercepting the clients requests, and responding appropriately to those requests. The concept behind such a mechanism is that if the requests were to go all the way to the original Web Server hosting the material, it might take some time for the web server to respond, as it might not be close to the client. Secondly it doesn't make sense to use the precious bandwidth, time and again for repeated requests of the same material. If such kind of content can be placed topologically closer to the client on some local proxy server, bandwidth and latency issues involved if fetching the data from the original server can be resolved to a certain extent and the Web Server can be relieved off some load.

Reference: *Web Caching.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/cache_switching.html

Can we cache each and every content request?

It's quite hard to cache all the content that's requested by the clients off the web. There is a certain intrinsic characteristic within the content, which allows it to be cached. Content that is dynamic in nature or in other words, that changes quite often cannot be cached. Content related to CGI scripts, Active Server pages cannot be cached. On the other hand content such as large, static objects that change infrequently such as GIF, JPEG images are suitable candidates for caching. Layer 5 switches have the ability to check the content of the packet, and then make a calculated decision of which server to approach, to pass on the request. For contents that are cacheable, the requests are diverted to the caches. For non-cacheable requests, the layer 5 switch tries to establish a session with the Web Server hosting the content.

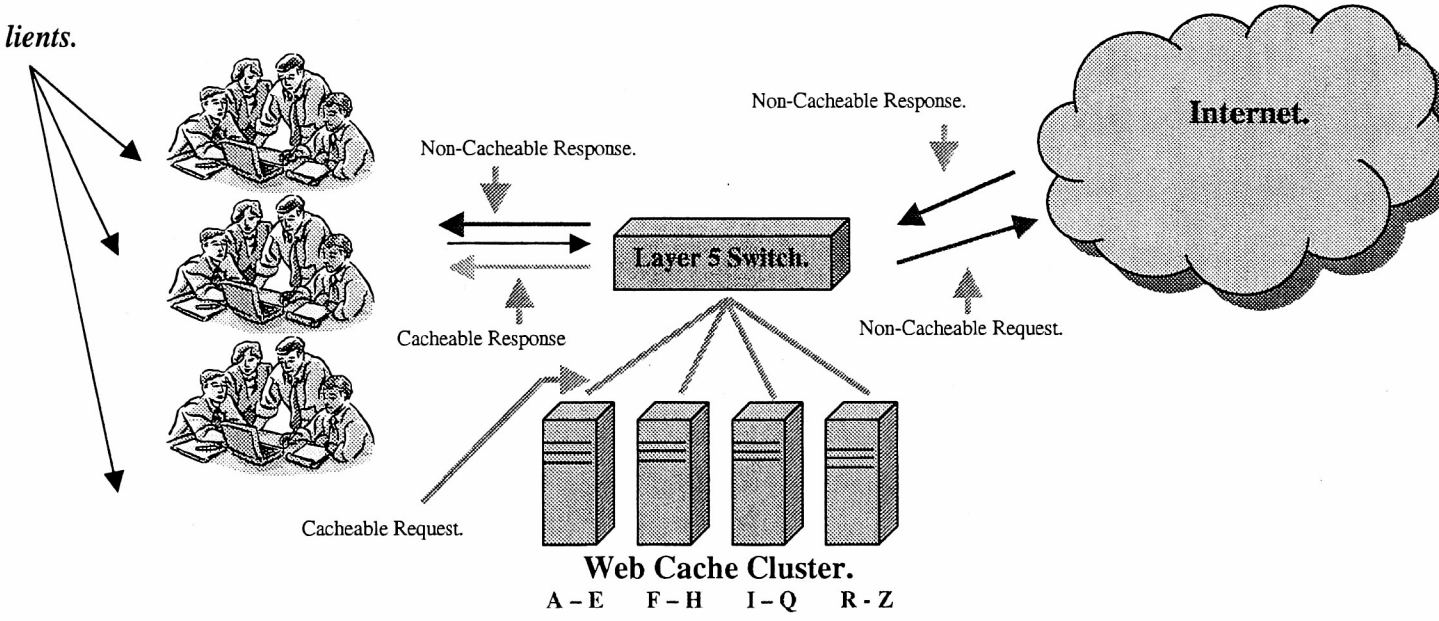


The diagram represents the use of smart and efficient network device (Layer 4 Switch) to redirect web traffic. The point of concern out here is that the Layer 4 switches cannot differentiate between HTTP traffic. The TCP port for Web traffic (HTTP traffic) is ***port 80***. All web applications use the same port number. Since the layer 4 switches cannot

differentiate between HTTP traffic, it transmits all requests, viz. cacheable as well as non-cacheable requests to the Cache Server. Sending non-cacheable requests to the Cache Server proves futile and can severely undermine its processing performance, because these requests are diverted to the main server that's hosting the content. The inability of layer 4 switch to differentiate between different types of web traffic / web applications, creates the need for switching to go to layer 5, i.e. the session layer of the OSI reference model.

Reference: *TCP level / Layer 4 Switching in the Network.*
http://www.terena.nl/tech/d2-workshop/d2cache99/transpcaching/sld014.htm

Web Caching Scenario – 2.



Due to the inability of layer 4 switches to look into port 80 (HTTP) traffic, the necessity for layer 5 switches becomes even more. Unlike in layer 4 switches where both cacheable as well as non-cacheable content (entire HTTP traffic) gets forwarded to the Cache server, Layer 5 switches take the microscope to a higher level. Layer 5 switches have the

ability to look further into the packet, check the content that's being requested by the client (cacheable/non-cacheable). This way the layer 5 switch learns what content is being requested, and is in a position to forward the request to the appropriate server.

Cluster Caching is becoming a strategic aspect of the networking infrastructure needed to support layer 5 switching. The need to deploy multiple caches arises due to the following aspects: -

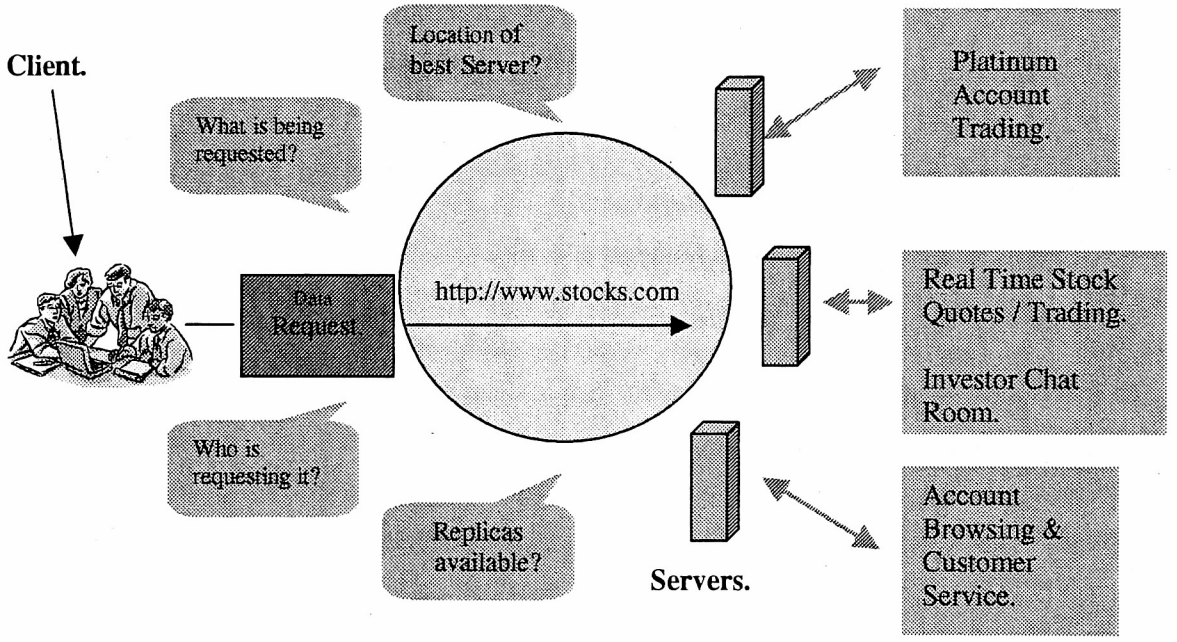
- *Redundancy:* Although it adds up to the fixed cost of the networking infrastructure, multiple caches are required to overcome the scenario of a single cache failure. If one cache fails, there needs to be a backup cache that will take care of its responsibilities. Having a cluster of caches takes care of this problem. If one cache goes down the other caches can partition the traffic load amongst them, and continue on with the processing mechanism.
- *Effective traffic management:* Organizing *Cluster caches* to support traffic according to Domain Names, leads to better traffic management for cacheable contents within the Cache Server.
- *Scalability:* This aspect happens to be quite important be it any kind of technology. The ability to make the existing networking infrastructure flexible enough to support additional traffic, is something that the network administrators need to be aware off. *To scale cache performance and support additional clients, connections, content and bandwidth at a particular location on the network, it becomes imperative add caches.* The traffic load then gets partitioned amongst the various caches.

Reference: *Optimizing Network performance through effective Web Cache management.* *http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/cache_switching.html#conclusion*

Web Network Service for E-Commerce Transactions.

E-Commerce transactions are becoming quite popular on the net today. More and more people are switching to on-line purchases as compared to retail purchases down the local store. Companies need to make sure that their web-sites continue to give optimum levels of performance at all times. A pleasant on-line shopping experience for the customer is the key in maintaining a competitive edge in the E-Commerce market of today.

Concept cycle behind Layer 5 switching Strategy.



Reference: *Layer 5 switching strategy.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html #building

Customers will desist from shopping on a site with slow response times or failed attempts to make purchases. There are two things that are quite important for web sites/networking devices (i.e. especially Layer 5 switch) to sustain consistent levels of business activity.

- Support for persistent "*sticky*" network connections. It becomes essential that the client is mapped onto the same server for the entire duration of the purchase

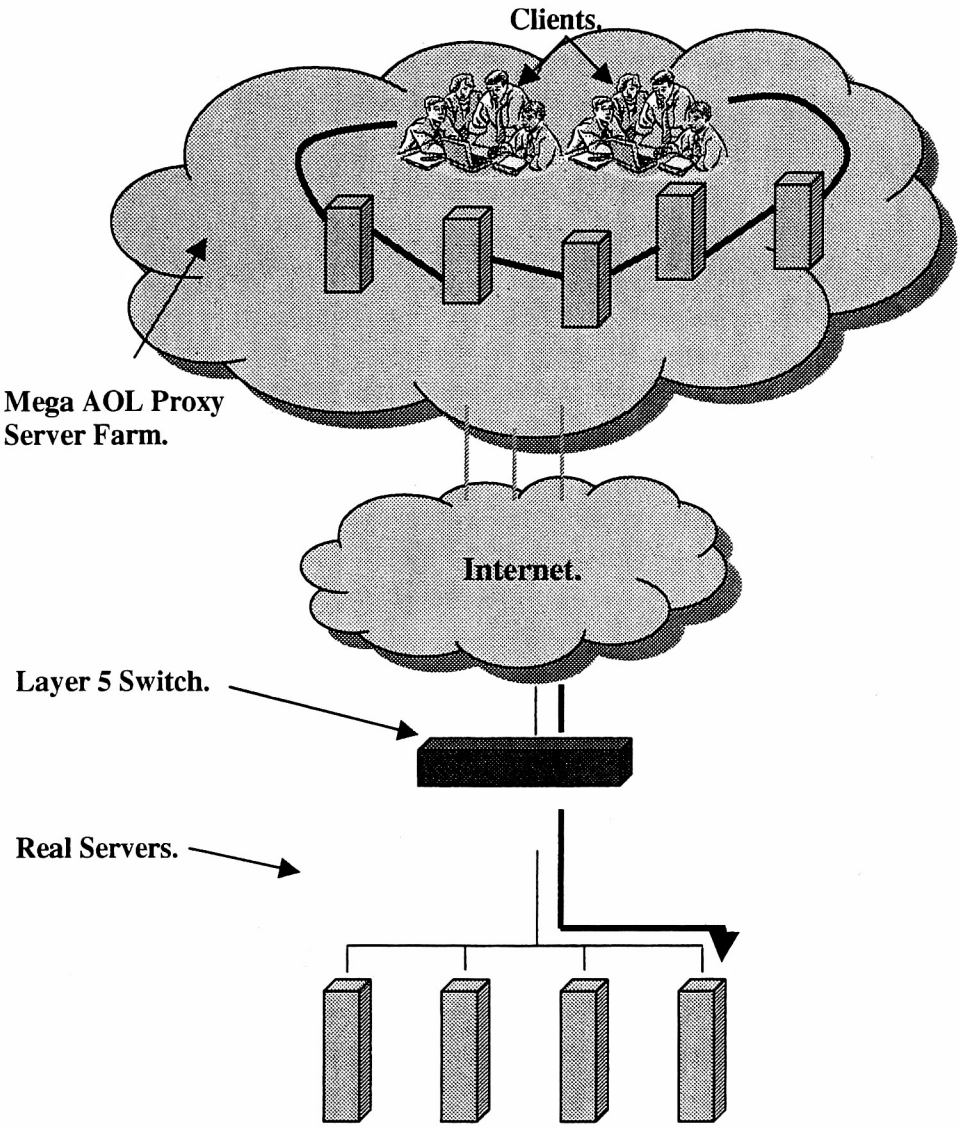
transaction so that the shopping carts are not lost before the purchase transaction is completed.

- *SSL (Secure Socket Layer)* transactions are quite important. Confidentiality needs to be maintained about information that's given on the Internet to conduct electronic transactions. Giving credit card number/accessing personal bank information needs to be encrypted when it is sent across the network. The SSL protocol was designed and developed by Netscape Communications. This protocol allows confidential traffic to be encrypted, which is quite essential to conduct electronic transactions on the Internet.

During load balancing operations on the network, each incoming network connection becomes completely independent of other network connections. There is a strong possibility of the client being diverted/load balanced to a different web server in the middle of the e-commerce transaction. The other server might not have an account of the client's shopping cart contents. This could lead to a severe fall in the revenue for the website and an unpleasant e-commerce shopping experience for the customer. In case of certain applications one wouldn't mind being load balanced to another server. For e.g. browsing the company site for some general-purpose information. But in case of e-commerce transactions, it becomes a necessity that a client be mapped to the same server for the entire duration of the e-commerce session.

Layer 5 switches/Content aware switches allow the e-business corporations to build web sites that are secure, reliable, scalable and that can support large surges in consumer traffic with ease. The technical aspects that are to be taken care off when building a web site depend on the following traffic scenarios: -

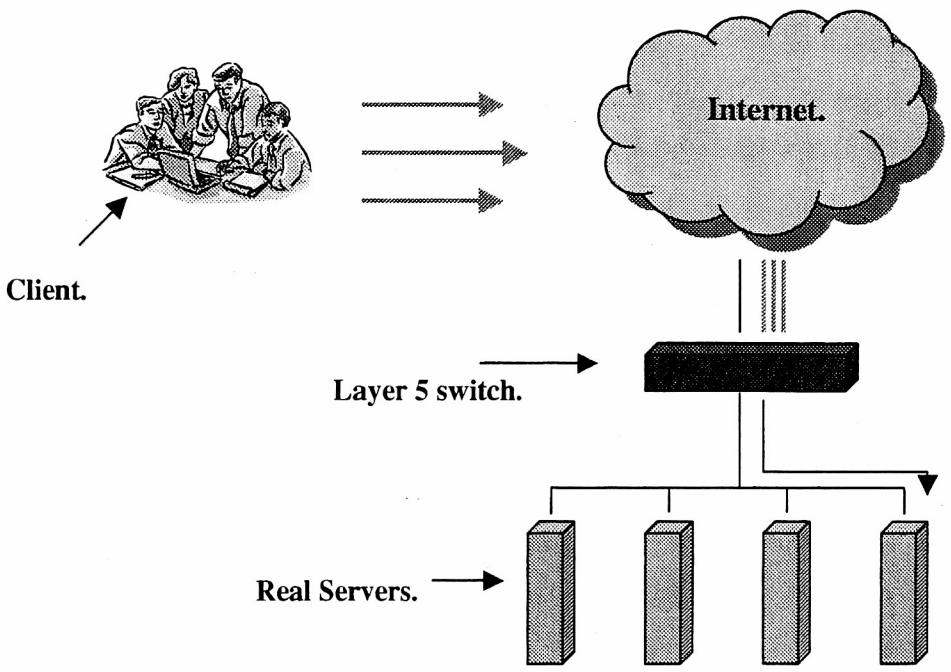
- ***Authenticated/Non-encrypted HTTP-based transactions:*** Many sites use authenticated/Non-encrypted HTTP-based transactions. Such might be the scenario when security aspects are least demanding. For e.g. a market research site allows its clients to use its resources online when they login. The client would enter the login ID and password and would gain access to the information. The main concern for the network administrator out here would be to see that the authenticated user does not lose the session connection. Session connection can be terminated if there is no activity for a certain period of time/session passes to a different server. Although it might be a security feature that the company introduced (session termination if no activity registered for a certain period of time), the clients might not appreciate the fact that they need to re-login once they are load balanced to a different server. The client can be mapped on to the same server throughout the life of the session through creating *Persistent "sticky" connections.* In the early stages, Load balancers provided persistent "sticky" connections by using the clients source IP address. So whenever the request came from the same client IP, the load balancer mapped the client back to the same server. This mechanism of creating persistent "sticky" connections became ineffective after ISP's started using Mega proxies (large farms of proxy servers). These proxy servers carry a virtual IP address. Source IP address in such a case is not an accurate method to determine a client, as the same source IP (virtual IP in case a client is coming from a mega proxy server – AOL) can be used by many clients. Secondly the source IP can change during the session if the proxy server goes down and the backup server is used to route the client's requests.



Reference: *Mega Proxy Server Persistence.*
http://www.sysmaster.com/support_tech_guide5.htm

Hence source IP address wasn't a reliable method of identifying the individual clients. This led to the need for a content switch (Layer 5 Switch). Content switches are able to forward data by looking into aspects such as file extensions, URL's, cookies. Switching on the base of cookie information is quite helpful as cookies can uniquely identify the clients and thereby maintain sticky connections.

Persistent "sticky" Connection- Cookie used to Map the Client to the same server.

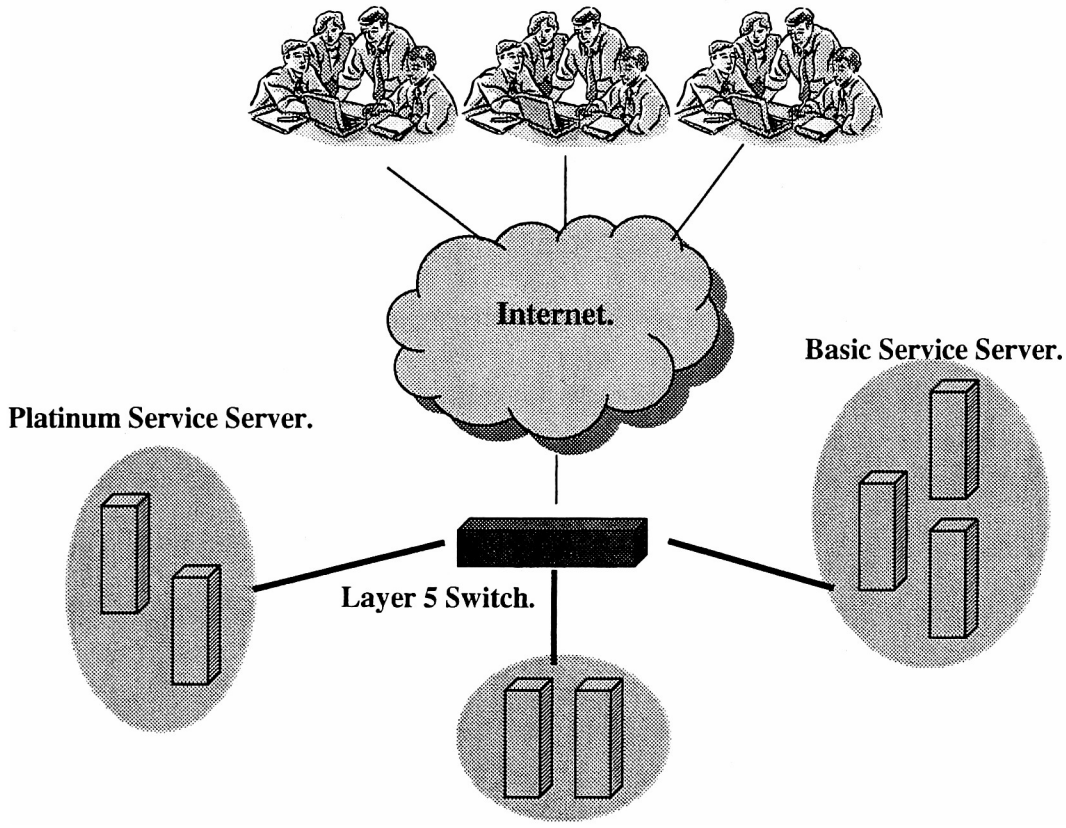


Reference: *What are Persistent Connections.*
http://www.sysmaster.com/support_tect_guide5.htm
Reference: *Authenticated Web Transactions.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario1

A cookie is a piece of text that the website stores on the client's hard disk. Cookie allows the site to store state information on the machine. Clients can be identified through the ID that the site stores in the cookie. Layer 5 switches can read the information that's inside the cookie, identify the clients on an individual basis and route them to the correct server. The amount of information that's stored in the cookie is dependent on the website itself. Some sites store more information. Cookie information is quite reliable during authenticated/non-encrypted web transactions, because even though the clients IP address might change during a session, the cookie information can be used to establish persistence between the client and the same server.

Reference: *How do web sites use cookies?*
http://www.howstuffworks.com/cookie3.htm
Reference: *How Internet Cookies Work?*
http://www.howstuffworks.com/cookie1.htm

Using Cookies to Prioritize Services for Premium customers.

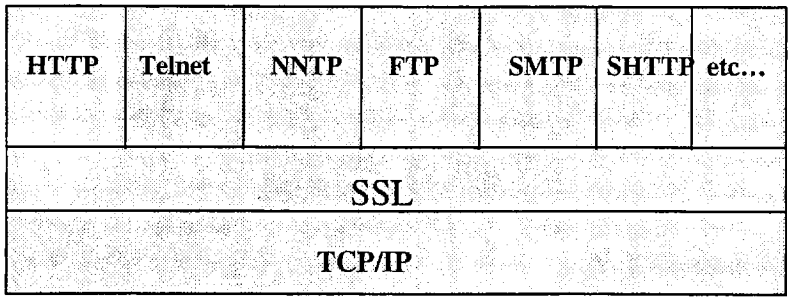


The mechanism for implementing priority amongst service requests is quite simple. The Layer 5 switch routes the client to the basic service server if it does not detect any cookie. When diverted to the Basic service server, the client completes the registration process. The client gets authenticated at the Basic service server, and gets the login ID and the password. The Basic service server then assigns a priority level for the client through some pre-determined criteria (e.g. associated business level from the client). It then assigns a Gold or a Platinum tag to the client. This tag value

is then stored in a cookie on the client's hard disk. The next time the client logs into the website, he/she will be routed to the appropriate server.

Reference: *Using Cookies to provide premium services.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#cookies

- ***End-to-end encrypted SSL (Secure Socket Layer) - based transactions:*** When e-commerce transactions are done, the highest levels of security are required to protect the transfer of data over the web. Mere authentication is not enough when conducting transactions on the web. Businesses such as banks and brokerage firms that allow their clients to use its resources require end-to-end encryption of data transfer. Such kind of security levels are pretty much mandatory for their business operations. SSL protocol is used to encrypt information that is being transferred between the client and the server. The SSL protocol is strategically layered between the application protocols and the connection protocols.



Reference: *Netscape's Secure Socket Layer.*
http://www.isc.rit.edu/~esp3641/ssl.html

When the information is sent from the client to the server, it has to traverse through several networks. When the data is in transit, any computer system that is in the middle of the transit path has the potential to access the sensitive client-server communication. Internet by itself does not provide any security features to encrypt the data. Netscape's SSL technology encrypts the data in such a manner that only the intended recipient is able to decrypt the information.

How Secure Socket Layer (SSL) works.

- *Exchanging "Hellos":* When a browser lands on a secure web site, the server that's hosting the web site sends a "hello request" to the browser. The browser in turn replies with a "client hello". On receiving the "client hello", the server responds with a "server hello". Exchanging these client/server hello messages (hello messages – a security handshake to start the TCP/IP connection) allows both, the client and the server to determine the level of security that's going to be used during the transmission session. Apart from exchanging the traditional hello messages, the browser and the server also exchange the session ID. This Session ID is unique for that particular session only.
- *Digital Certificate:* After exchanging the initial hello messages the browser asks for the server's "digital certificate". The digital certificate is basically a form of ID verification between the server's public key and the server's identification. The digital certificate is issued by a certificate authority, such as RSA data Security Inc or VerSign Inc. Each certificate issued by the certificate authority is unique and verifies a company's identification. The digital certificate that's issued for an on-line company contains the following:

  (a) *Certificate issuer's name,*

  (b) *The entity for whom the certificate is being issued i.e. the server,*

  (c) *The public key of the server.*

- *Sharing the key:* After checking the server's digital certificate, the browser uses the information in the digital certificate to encrypt the information and sends it to the

server in a format that only the intended server can understand. The browser and the server now create the master key, through which they can communicate with each other in an encrypted fashion. This master key is session dependent. Once the session is over, the key becomes useless. This entire process is re-performed when the browser and the secure server establish a session again.

Reference: *SSL - How does Secure Socket Layer Work.*
http://www.isc.rit.edu/~esp3641/ssl.html
Reference: *SSL – How SSL (Secure Socket Layer) Encryption Work.*
http://www.videoheadcleaner.com/ssl01.htm
Reference: *The Secure Socket Layer Protocol.*
http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/ssl.html

Persistent "sticky" connections are required during SSL end-to-end transactions. Cookies aren't helpful in such a scenario. A Layer 5 switch cannot read into the cookie information located in the HTTP header because the session traffic is encrypted. It therefore needs some other mechanism through which a sticky connection can be achieved between the client and the server session.

Reference: *Secure SSL transactions.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario2

During SSL transactions, the Layer 5 switch uses the SSL session ID to create a sticky connection between the client and the server. The SSL session ID is unique for each session and hence the client can be mapped onto the same server.

- ***Authenticated/encrypted HTTP-based transactions:*** Such transactions are basically hybrid transactions that involve authenticated HTTP and encrypted SSL connections. As the name suggests, a part of the transaction is non-secure and the other part is a secure transaction. Such kinds of transactions are quite common during a typical e-commerce session. The non-secure transaction could be when the client is merely

browsing the catalog and selecting the items that he/she intends to purchase. The items that are selected get added onto the shopping cart. When the client wishes to make a purchase he/she clicks the buy button. The site will ask for the client's identification (i.e. an existing user if the client has created an account with the site or new a user, if the client is coming to the site for the first time). As soon as the client gives this information a new session (SSL) is established between the client's browser and the web-server. All data transfer on this session is encrypted as it takes place over SSL.

Reference: *Hybrid Transactions using HTTP and SSL.*
http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario3

HTTP/1.0 is a stateless/connectionless protocol. This means that once the request by the client's browser for a web page has been satisfied by the Web-server, the connection between the client's browser and the Web-server is closed. Lets take a granular approach to the events that take place when the client requests a web page: -

1. An HTTP session is established between the client's browser and the Web-server hosting the Website. To make it more granular, two sessions get established. One session is between the client's browser and the Layer 5 switch, and a second session between the Layer 5 switch and the Web-server hosting the site.
2. The client's browser then sends an HTTP request.
3. The Web-server then replies back to the client's browser. The reply could be the requested web page that the client needs, or an error message saying that the page requested could not be found.
4. The connection between the client's browser and the Web-server is closed.

Reference: *Session Tracking on the Web.*
http://www.internettg.org/newsletter/mar00/workshop_session_management.html

The very fact that HTTP is a stateless protocol might lead to problems for e-commerce applications. It would be quite surprising to know that it isn't an easy task for the Web-server to keep a track of all the transactions that a client has had with it. Such an aspect would create issues with web applications involving shopping carts, and especially when the transaction flips from HTTP to SSL. The question that needs to be answered is how does the Web-server know what you were buying i.e. how does the Web-server keep a track of your shopping cart? This issue is taken care off through different Session Tracking mechanisms that the Web-servers can use. *Session Tracking is a mechanism in place to maintain the state of a series of requests originating from the same client over a period of time.* This way the Web-server can keep a track of all the selections a client has made in the shopping cart.

Reference: *What is Session Tracking.*
http://www.apl.jhu.edu/~hall/java/Servlet-Tutorial/Servlet-Tutorial-Session-Tracking.html
Reference: *Saving Client State - Session Tracking.*
http://java.sun.com/docs/books/tutorial/servlets/client-state/session-tracking.html

Session Tracking Mechanisms.

- ***Cookies:*** HTTP cookies can be used to store information about a shopping session. The Web-server can then use the cookies (information pertaining to the session – Session ID) to extract the session information and keep a constant track of the client's shopping cart. This has been by far the most common and the easiest way to track client sessions. The cookies can be created, read and modified on the server-side using CGI scripts or via servlets. The problem with this mechanism is that Web-servers cannot always rely on cookie information to keep a track of the client's

sessions. If the client disables the cookies in the browser, this method won't work. Secondly, it isn't a good method to store sensitive information on cookies.

- ***URL Rewriting:*** Even if the browsers don't accept cookies, the Web-server can still track the client sessions by making sure that every URL/link the Web-server sends back to the client's browser has the session ID appended to it. Through this mechanism the Web-server can associate the session identifier with the data it stored for that particular session. This method has its share of problems. Lot of server-side processing needs to be done to make sure the URL that is being sent to the client's browser has the session information appended to it. This method although straightforward, requires lot of tedious processing.
- ***Hidden form fields:*** This mechanism of session tracking is achieved by adding fields to an HTML form that aren't displayed by the client's form. The data that's stored in these hidden fields is sent to the Web-server along with other information from other Form fields such as text fields, radio buttons, check boxes etc. These hidden fields contain the NAME/VALUE pair, where the NAME refers to the session information and the VALUE refers to the username. The Web-server uses this information (NAME/VALUE pair) to keep a track of the client's session information as he/she moves from page to page. This technique is supported by all browsers, but works only for dynamically generated forms.

Reference: *Safe Session Tracking – Mechanisms for Tracking Sessions.*
http://www.sdmagazine.com/documents/s=733/sdm0103h/0103h.htm

Server Persistence.

Apart from having knowledge of prior client-server sessions it is quite important to know the port number of the Web-server to which the prior sessions were directed.

Server persistence is necessary. It's quite important to have all subsequent sessions of the client's browser directed to the same Web-server. If the client's request gets load balanced to a different Web-server amongst the virtual server group, the other server might not have knowledge of the client's prior transactions.

The company might have a few servers at port 80 and may direct requests to transaction servers that might be situated on different ports. It isn't important to keep Web-servers at port 80. One could have a Web-server at a different port, for example port 921 or any other port that is not in use. If a web site has the URL as www.abc.com, and has a transaction server situated at port 921, the layer 5 switch could establish a session with the transaction server at port 921 with the URL http://www.abc.com:921. The port number *(after the colon (i.e. 921) refers to the actual server within the virtual server group)* has to be included in the URL if the layer 5 switch needs to establish a session with that particular Web-server. If the port number is not specified, the session between the layer 5 switch and the Web-server will get established with the server that's situated at port 80. The same is also true in case of secure transactions. Companies like to differentiate their servers based upon the tasks. Network designers wouldn't want to have secure transactions being performed on transaction servers. Secure transactions need to be done on secure servers. A similar concept could be applied to secure servers wherein a couple of servers dedicated for secure transactions, could be grouped together to form a virtual secure server. A Layer 5 switch will have to maintain persistent connection with the actual secure server amongst the virtual server group to oversee the completion of a successful/pleasant e-commerce transaction.

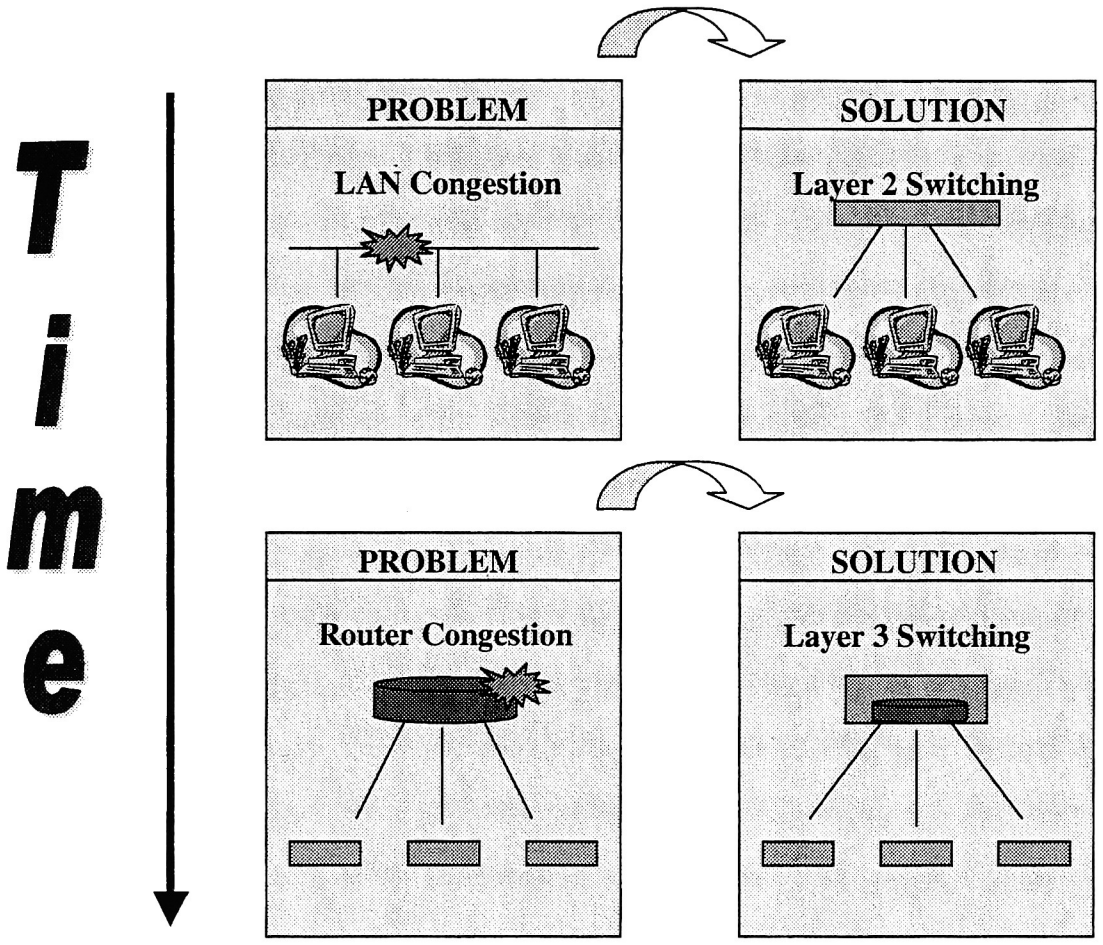
Reference: *How Web-servers and the Internet work – How ports work.*
http://www.howstuffworks.com/web-server5.htm

Better Solution to Session Tracking (HTTP/1.1)

People at the World Wide Web consortium (W3C) were aware of this problem in HTTP/1.0 and proposed a new version HTTP/1.1, which apart from other technical enhancements supports *persistent connections*. With persistent connection feature in place, the connection between the client's browser and the Web-server remains open until the session times out by itself or is explicitly closed by the client. Since the same connection can be used for the entire life of the session to conduct all the client-server data communication, it makes a lot easier for the Web-server to keep a track of the client session.

***Reference**: HTTP/1.1 Improves Web Performance and Security.*
http://www.w3.org/1999/07/HTTP-PressRelease
***Reference:** A Better Solution to Session Tracking.*
http://www.internettg.org/newsletter/mar00/workshop_session_management.html

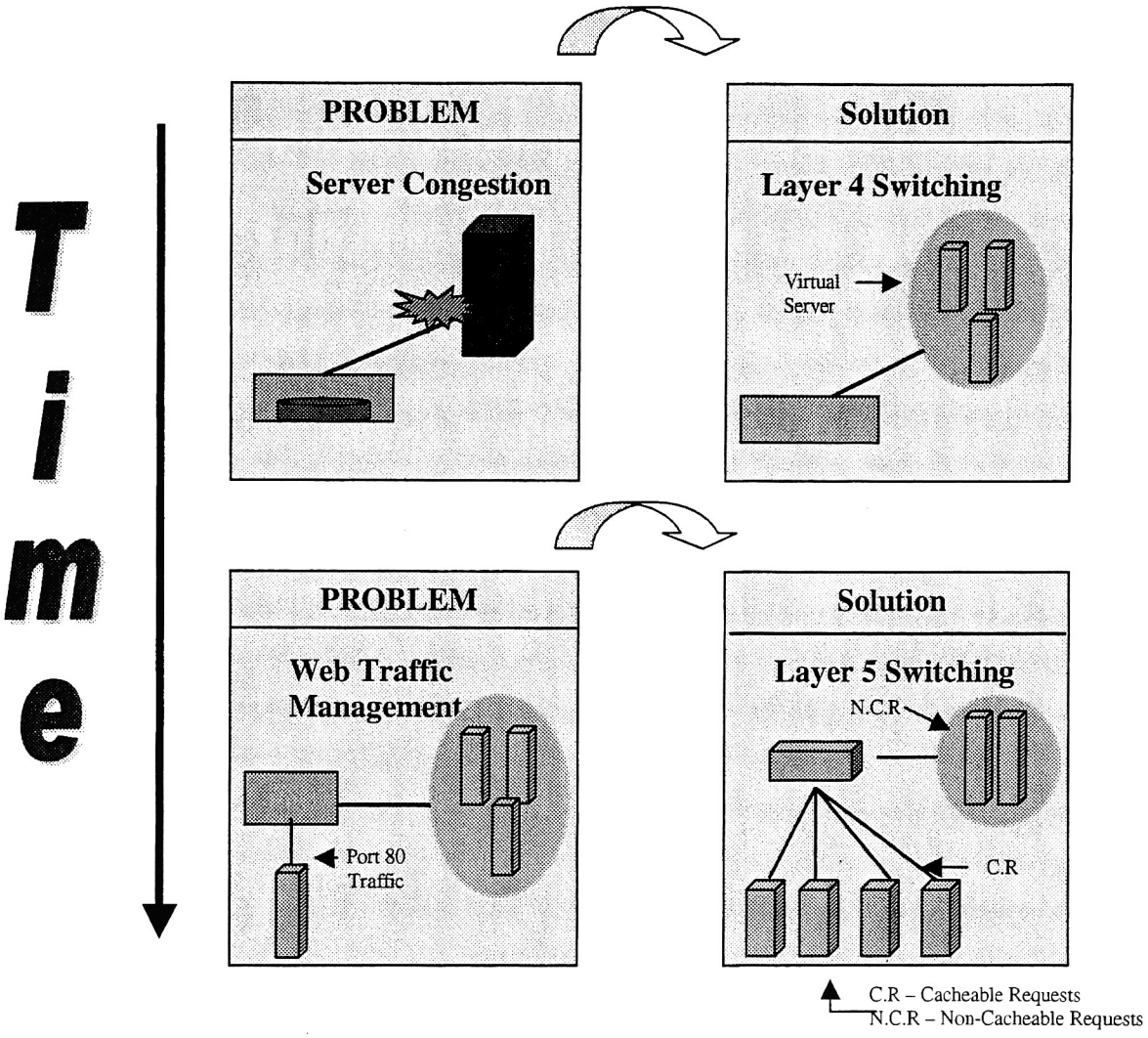
Conclusion.



Layer 2 Switching was introduced to resolve the bandwidth and the latency issues associated with the most common LAN media - the traditional Ethernet. Layer 2 Switching works around the problem of LAN congestion by making collision domains within the LAN segment, thereby preserving the network and bandwidth utilization and lowering the latency factor.

Layer 3 Switching was introduced to resolve the Router congestion problem. Packet processing in a router takes place at a CPU level, which slows down the forwarding operation when access lists are turned on. Layer 3 Switches implement the forwarding mechanism via ASIC. It enables wire speed performance in inter LAN communication.

Conclusion continued ....



Layer 4 Switching resolves the Server congestion problem. It lays down rules for load balancing of network traffic amongst the servers. Network traffic flow is analyzed out here. Requests are sent to different servers based on the traffic type. Preferential treatment is given to time sensitive/mission critical applications.

Layer 5 Switching takes care of an important aspect of traffic management that Layer 4 Switching cannot achieve. Layer 5 Switches are capable of analyzing port 80 traffic and sending requests to appropriate servers. This stems from the fact that the Layer 5 Switches can differentiate between cacheable and non-cacheable web-content.

References.

1. LAN Switching.
URL: ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm

2. LAN Switching - Faster CPU's
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs0./10.htm

3. LAN Switching - Multitasking.
URL:http://www.pcwebopedia.com/TERM/M/multitasking.html

4. LAN Switching - Multitasking.
URL:http://burks.brighton.ac.uk/burks/foldoc/83/75.htm

5. LAN Switching - Network Intensive Applications.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs0./10.htm

6. Switching Concepts and LAN Switching Technologies. - Layer 2 Switching in the Protocol Stack. Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

7. Switching by Analyzing the Destination Address.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm#xtocid191881

8. Address learning.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm.

9. Solution to loops in a network.
URL:http://support.baynetworks.com/library/tpubs/html/router/soft1000/bridge/2950A-19.html

10. Spanning Tree Algorithm.
URL:http://support.baynetworks.com/library/tpubs/html/router/soft1000/bridge/2950A-19.html

11. Spanning Tree Algorithm.
URL:http://www.ciscoworldmagazine.com/monthly/1999/12/spantree.shtml

12. Link State Routing Protocols.
URL:http://www.freesoft.org/CIE/Topics/118.htm

13. Link State Routing Protocols.
URL:http://burks.brighton.ac.uk/burks/foldoc/8/67.htm

14. Overview of common routing protocols. - Link State Routing Protocols.
URL:http://www.wireless-nets.com/whitepaper_routing.htm

15. Layer 2 Switching process.
URL:http://www.alliedtelesyn.co.nz/support/rapier/rapier221/switch.pdf

16. Switching Technology - Cut Through Switching.
URL:ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm#cut

17. Switching Technology - Cut Through Switching.
URL:http://www.anixter.com/techlib/whiteppr/network/d0504p06.htm

18. Switching Concepts and LAN Switching Technologies. - Cut Through Switching.
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

19. Switching Technology - Store and forward switching.
URL:http://www.anixter.com/techlib/whiteppr/network/d0504p06.htm

20. Switching Concepts and LAN Switching Technologies. - Store and forward switching.
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

21. Buffer Concepts - Input and Output Buffering.
URL:ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/lan_switching/index.htm#buffer

22. Switching Concepts and LAN Switching Technologies. - Input and Output Buffering
Metz, Christopher Y., IP Switching Protocols and Architectures, McGraw-Hill, 1999.

23. Functions of Layer 2 Switching.
URL:http://www.certifyexpress.com/cisc/resources/2switching.shtml

24. Benefits of Layer 2 Switching.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs010.htm

25. Layer 3 switching.
URL:http://www.pulsewan.com/data101/layer3_switching_basics.htm

26. Layer 3 Switching. Re-Inventing the Router. The Technology Guide Series at techguide.com.
URL:http://www.techguide.com/html/3switch.pdf

27. The key to greater performance and application control - Packet switching.
URL:http://www.enterasys.com/products/whitepapers/multilayer/

28. TCP/IP Protocol Suite - Routing Information Protocol.
URL:http://www.networksorcery.com/enp/protocol/rip.htm

29. IGRP Protocol Characteristics.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

30. OSPF (Open Shortest Path First) Background.
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm#17394

31. Cisco Layer 3 Switching Demystified.
URL:http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/l3c85_wp.htm

32. Cisco – HSRP Background and Operations.
URL:http://www.cisco.com/warp/public/619/hsrpguide1.html

33. HSRP, Hot Standby Router Protocol.
URL:http://www.networksorcery.com/enp/protocol/hsrp.htm

34. HSRP, Hot Standby Router Protocol. RFC - 228.
URL:http://www.faqs.org/rfcs/rfc2281.html

35. Dynamic Host Configuration Protocol (DHCP).
URL:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213894,00.html

36. DHCP.
URL:http://www.webopedia.com/TERM/D/DHCP.html

37. Dynamic Host Configuration Protocol (DHCP) FAQ.
URL:http://www.dhcp-handbook.com/dhcp_faq.html#widxx

38. Simple Network Management Protocol (SNMP).
URL:http://www.cisco.com/warp/public/535/3.html

39. Simple Network Management Protocol (SNMP).
URL:http://webopedia.internet.com/TERM/S/SNMP.html

40. File Transfer Protocol (FTP).
URL:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213976,00.html

41. Network Time Protocol (NTP).
URL:http://toi.iriti.cnr.it/uk/ntp.html

42. NTP.
URL:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci283988,00.html

43. Coordinated Universal Time.
URL:http://whatis.techtarget.com/definition/0,,sid9_gci213612,00.html

44. Access control list (ACL).
URL:http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213757,00.html

45. IP Passport (Accelar) - When to use switches and when to use routers.
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

46. Switch Vs Router.
URL:http://www1.ietf.org/mail-archive/ietf/Current/msg11453.html

47. Can Layer 3 switching increase bandwidth?
URL:http://www.nwfusion.com/newsletters/lans/0601lan2.html

48. Layer 3 switching – (ASIC) Chip-Based Functionality.
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

49. Benefits of Layer 3 switching.
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

50. Multi-Protocol over ATM (MPOA) Overview.
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/switch_c/xcprt7/xcmpoa.htm

51. Article on Layer 3 Switching- The enabler of IP-optimized Networking.(MPOA)
URL:http://www.nortelnetworks.com/solutions/financial/collateral/sept98_l3_switch_v1.pdf

52. MPLS and Label Switching Networks - Why use Label Switching.
Black, Uyless D., MPLS and Label Switching Networks, Prentice Hall Series, 2001

53. Multiprotocol Label Switching (MPLS).
URL:http://www.iec.org/online/tutorials/mpls/topic03.html?Next.x=41&Next.y=12

54. Multiprotocol Label Switching (MPLS).
URL:http://www.webopedia.com/TERM/M/MPLS.html

55. Multiprotocol Label Switching (MPLS).
URL:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214350,00.html

56. Article on Layer 3 Switching- the enabler of IP-optimized Networking. (MPLS)
URL:http://www.nortelnetworks.com/solutions/financial/collateral/sept98_l3_switch_v1.pdf

57. Layer 3 Switching – Need for layer 3 switches.
URL:http://www.mouse.deamon.nl/ckp/lanwan/13switch.htm

58. Layer 3 switching.
URL:http://www.cisco.com/warp/public/779/largeent/learn/technologies/L3_switching.html

59. Layer 3 Switch Vs Traditional router.
Regis, Bates J, Jr and Kimmel Zeecil.., Nortel Networks Layer 3 Switching, McGraw-Hill, 2001

60. OSI Model Layers
URL:http://geocites.com/SiliconValley/Monitor/3131/ne/osimodel.html

61. The Seven-Layer Model. – The Transport Layer
URL:http://www.rad.com/networks/1994/osi/transp.htm

62. The OSI Seven-Layer Model- Common suite of TCP/IP protocols
URL:http://www.netc.org/network_guide/c.html

63. Layer 4 Switching.
URL:http://www.msic.com/ebusiness/convergence/layerswitch.shtml

64. Well known port numbers.
URL:http://www.freesoft.org/CIE/RFC/1700/4.htm

65. Layer 4 switching.
URL:http://www.comtest.com/tutorials/layer4.html

66. Layer 4 Switching: Hype or Hope
URL:http://www.sterlingresearch.com/library/library/05_98layer4_switching.html

67. Layer 4 Switching.
URL:http://www.comtest.com/tutorials/layer4.html

68. Layer 4 Switching.
URL:http://www.tbg.com/Public/WhitePapers/L4_switching.html

69. Layer 4 switching.
URL:http://www.comtest.com/tutorials/layer4.html

70. Layer 4 switching: The magic combination.
URL:http://www.nwfusion.com/newsletters/lans/0215lan1.html

71. Layer 4 switching.
URL:http://www.idg.net/crd_switch_67600.html

72. Analyzing the packet - IP Packet Header.
URL:http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html

73. Layer 4 Switching is for real.
URL:http://www.nwfusion.com/forum/0208layer4yes.html

74. The Ins and Outs of Layer 4 Switching. Dr Shirish Sathaye – Alteon Networks.
URL:http://www.nanog.org/mtg-9901/ppt/alteon/sld011.htm

75. The Ins and Outs of Layer 4 Switching. Dr Shirish Sathaye – Alteon Networks.
URL:http://www.nanog.org/mtg-9901/ppt/alteon/sld006.htm

76. Benefits of Application-Level Control. – QoS, Security and Accounting.
URL:http://www.enterasys.com/products/whitepapers/multilayer

77. RMON (Remote Monitoring).
URL:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm

78. RMON Groups.
URL:http://www.rmon.co.uk/html/rmon_groups.htm

79. Benefits of Layer 4 Switching - Examining Layer 4 Information.
URL:http://www.tbg.com/Public/WhitePapers/L4_switching.html

80. Session Layer - OSI seven layer model.
URL:http://www.geocities.com/SiliconValley/Monitor/3131/ne/osimodel.html

81. The Session layer.
URL:http://www.rad.com/networks/1994/osi/session.htm

82. Layer 5 / Session layer switching.
URL:http://www.cc.gatech.edu/~wooylee/Layer-5switch.pdf

83. Parsing with precision – Sophisticated traffic management.
URL:http://www.nwfusion.com/research/2000/0501feat2.html

84. URL Parsing
URL:http://www.f5networks.com/solutions/whitepapers/http.pdf

85. Content Smart Cache Switching.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/cache_switching.html

86. TCP level / Layer 4 Switch load balancing in the Network.
URL:http://www.terena.nl/tech/d2-workshop/d2cache99/transpcaching/sld014.htm

87. Web Caching.
URL:http://www.cs.wisc.edu/~cao/WISP98/html-versions/anja/proxim_wisp/node2.html

88. Secure E-Commerce transactions.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html

89. Optimizing Network performance through effective Web Cache management.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/cache_switching.html#conclusion

90. Layer 5 switching strategy.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#building

91. Mega Proxy Server Persistence.
URL:http://www.sysmaster.com/support_tech_guide5.htm

92. What are Persistent Connections?
URL:http://www.sysmaster.com/support_tect_guide5.htm

93. Authenticated Web Transactions.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario1

94. How do web sites use cookies?
URL:http://www.howstuffworks.com/cookie3.htm

95. How Internet Cookies Work?
URL:http://www.howstuffworks.com/cookie1.htm

96. Using Cookies to provide premium services.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#cookies

97. Netscape's Secure Socket Layer.
URL:http://www.isc.rit.edu/~esp3641/ssl.html

98. Secure Socket Layer - How does Secure Socket Layer Work.
URL:http://www.isc.rit.edu/~esp3641/ssl.html

99. The Secure Socket Layer Protocol.
URL:http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/ssl.html

100. Secure Socket Layer (SSL) Protocol - How SSL (Secure Socket Layer) Encryption Work.
URL:http://www.videoheadcleaner.com/ssl01.htm

101. Secure SSL transactions.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario2

102. Hybrid Transactions using HTTP and SSL.
URL:http://www.knowware.co.uk/ArrowPoint/solutions/whitepapers/secure_scalable_ecommerce.html#scenario3

103. Session Tracking on the Web.
URL:http://www.internettg.org/newsletter/mar00/workshop_session_management.html

104. What is Session Tracking?
URL:http://www.apl.jhu.edu/~hall/java/Servlet-Tutorial/Servlet-Tutorial-Session-Tracking.html

105. Saving Client State - Session Tracking.
URL:http://java.sun.com/docs/books/tutorial/servlets/client-state/session-tracking.html

106. Safe Session Tracking – Mechanisms for Tracking Sessions.
URL:http://www.sdmagazine.com/documents/s=733/sdm0103h/0103h.htm

107. How Web-servers and the Internet work – How ports work.
URL:http://www.howstuffworks.com/web-server5.htm

108. HTTP/1.1 Improves Web Performance and Security.
URL:http://www.w3.org/1999/07/HTTP-PressRelease

109. A Better Solution to Session Tracking.
URL:http://www.internettg.org/newsletter/mar00/workshop_session_management.html