Ind Jour Math & Comp Sc. Jhs. Vol. II - Pt I, 2013 Pg 1- 8

"Exploring the efficiency of IGMP Snooping by query snooping algorithms with various indexing."

Dr. U.S.Pandey, Pankaj Dadhich
School of Open Learning, Delhi University, Delhi,
Shri Jain Kanya Mahavidhyalay, M.G.S.University, Bikaner,
uspandey1@gmail.com, pankajdadhich1@gmail.com
Recceived on 26/2/2012

ABSTRACT : IGMP snooping is mostly useful in the VPLS instance where a small number of routers are attached and the majority of access circuits are Ethernet switch based. The snooping device is transparent. IGMP packets are read and then forwarded upstream to the multicast router, monitoring IGMP traffic and stop sending multicast traffic when a host leaves. it does not participate in the IGMP host messaging and promiscuously listens to transactions between clients and routers to determine when join/leave processing is required to a downstream host.

By default, the switch will only forward traffic out those ports with multicast clients.

Snooping switch "snoops" the join messages which ports will receive the multicast data.

The multicast router sends out periodic IGMP snooping Querier to all VLANs and added in to the forwarding table and periodically monitor each end device in the network which multicasts they wish to receive, refreshing the IGMP multicast/port associations. It is known as IGMP reports.

ORIGINS OF THE WORD

Snooping is derived from the German word schnooben, which was invented by Hitler in 1927. It means 'watching your neighbors to see if they are being un-German' and was brought to America and England by German spies just prior to the end of WWII. As they had no way of returning to their homeland, the spies gave up faking accents and dropped back into their native German ones. In England, during the Great Witch-Hunt of the 1930s schnooben was incorperated as the word 'snooping' we know and love today. In America, however, schnooben took a different path and was transformed into slang meaning 'I sleep where I can see my neighbors'.

Snooping in the bridged world refers to a bridge control plane picking up certain frames not addressed to it, processing the frame, and only then forwarding it. Snooping is typically done for the purpose of optimizing forwarding or for security reasons.

Snooping is the effective approach for monitoring in positive and negative manner. In past this approach use for negative aspect beause in general human tendency to have curiosity in the other's personal matters, And at the Internet, this tendency highly dynamically grows. So better be alert. Snooping refers to the act of unauthorized access to others database and personal information. It also covers the act of parting with confidential information (such as customer's data) for the benefit of a third party.

Snooping may not have criminal impact or assault, but nevertheless loosing one's privacy can be equally disturbing. It is not a subject to know that your associates: parents, boss, government and law enforcing agencies included are all preparing to dig into your inbox, browser and your computer? They may have their own reasons for doing so but ultimately it's your privacy that's being plundered, and this process is called snooping.

Snooping: Online Privacy

Snooping, in a security perspective, is unauthorized access to another person's or company's data. The practice is similar to listening in but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage; governments may snoop on individuals to collect information and prevent crime and terrorism. Watch out the e-mail entering your inbox might be loaded with software that lets marketers track your moves online, and you may not even be aware that you've been bugged.

Almost all Web sites plant bits of code called "cookies" on consumers' hard drives for regular invigilation of Internet pages for returning visitors and better target ads. Now, enhanced messages that share the look and feel of Web pages are being used to deliver the same bits of code through email, in many cases without regard for safeguards that have been developed to protect consumer privacy on the Web. However cookies can't be a serious threat to your privacy since they can be barred. Some e-mail programs already include settings allowing consumers to block cookies. Microsoft's Internet Explorer 6.0, for example, offers controls for cookies on the Web and via the company's Outlook and Outlook Express e-mail programs. Turning on the "prompt for cookies" setting can reveal the stunning extent of the problem, unmasking unsolicited HTML e-mail messages that try to lay down cookies on a hard drive. Have you experienced this? You buy a mobile connection filling a form containing your personal details. Within hours of activation of your connection, the first person to call you on your mobile will be none other than a salesman or insurance advisor or a marketing representative. Ask him from where he got your number and he'll hang up. You need not wonder! It's a part of "terms and conditions" that your cell operator (or any other business firm for that matter) insist that it's entitled to use your personal information.

To be sure, some retailers are starting to refer to e-mail monitoring in privacy policies. Amazon.com, for example, mentions that it may use tracking methods via e-mail to determine preferences for future communications. Still, privacy advocates said e-mail privacy practices are largely under-disclosed compared with other media such as the Web. Well. For all the bluster about online privacy, most of us don't care that much. Consider:

1. A top-100 Web sites, have a privacy policy but .039 % of people going through its Privacy policy while signing up. It is due to lake of knowledge.
2. E-tailers such as LLBean.com, Ticketmaster Online-Citysearch and Bloomingdales.com tell you right up front that your data is given to partners. And people buy things from them all the time.

Most of us are not serious about online privacy. Mainly because it hasn't caused much damage compared to the impact of virus, cyber stalking and other dangerous devils of the internet. But the irritation and mental disturbance it can give can be equally severe.

Snooping: Data Protection

The importance of data privacy is growing. In the past, it was possible to maintain reasonable control over who could view data because access tended to be available only through individual systems and applications with a known set of users. Rarely was there a need to distinguish between those who could update data and those who could view it, as they were usually be the same people. As a result, security breaches were relatively rare.

But advances in technology have brought about new problems. Data can now be downloaded locally from spreadsheets and databases, various middleware products can transfer data between applications or to local datamarts, and data warehousing has made it possible to assemble data accessible by many people in an organization. In most cases, these technologies were deployed without any thought about security.

The internet further extended the use of shared data through credit card details and e-mail addresses, and increased the importance of data privacy. Few people are happy at the idea of their e-mail address being freely distributed and everyone who enters their credit card details on the internet expects the information to be held securely. Will it be? Is the question.

Threats to data protection :

1. **Demolition -** Physical demolition of essential information assets using predictable weapons.
2. **Disturbance -** Electronic disturbance using non-formal weapons, viz. EMP (electromagnetic pulse), DEW (directed energy weapons), etc.
3. **Data manipulation-** Computer viruses, worms, Trojans, and other malicious software.
4. **Data prevention -** Sniffers and other 'snooping' techniques to prevention confidential information.
5. **Nicking -** Malicious software embedded surreptitiously in systems.

Firewalls are what comes to one's mind on the thought of security but a firewall, however, is not secure. There isn't a firewall that a group of experts can't get around, despite the increasing sophistication of firewall defenses. In the perpetual war between hackers and defenders, the defenders have to be lucky all the time, hackers just once.

State sponsored Snooping

Previous 3 years net service providers in the UK were obliged to carry out surveillance of some customers' web habits on behalf of the police.

Controversial laws passed in 2000 oblige large communications companies to install technology that allows one in 10,000 of their customers to be watched.

The controversial Regulation of Investigatory Powers Act was passed in October 2000 and gave law enforcement agencies sweeping powers to snoop on the

electronic lives of citizens. In simplest words it's the internet equivalent of a telephone tap.

It also demands that service providers start monitoring a customer within 24 hours of being told that the police or other investigation agencies want to snoop on them.

The information gathered about what people look at on the web, the content of e-mail messages and their phone conversations would be passed to the police or a government monitoring station.

The bush administration in U.S also has similar law in force, with an official purpose of monitoring terrorist activities. FBI (Federal Bureau of Intelligence) has its own infamous Internet surveillance program called Carnivore.

Security Aspect

In security sector we can use snooping approach for Universe, world, national, personal, cultural, social, natural disasters, terrorism, moral ,combating serious crime, climate change (Rising ocean water levels could threaten coastal bases at home and abroad, and increasing storm activity, droughts, violent weather) monitoring.

Technical Aspect

Snooping switch provides to look or pry especially in a sneaking or meddlesome manner.

1. Normally bridges forward frames except those addressed to its management entity or those addressed to the well-known bridge address. Snooping in the bridged world refers to a bridge control plane picking up certain frames not addressed to it, processing the frame, and only then forwarding it.
2. Snooping is typically done for the purpose of optimizing forwarding or for security reasons.
3. Creates FC point-to-point links within the Ethernet LAN. This switch has complete point-to-point control over the traffic when a device inserts into fabric or release from the fabric. Allows auto-configuration of ACLs based on name server information read in the FIP frames.
4. This switch also ensures that device is using their assigned addresses and presents various types of malicious anomalous behavior.
5. IGMP snooping switch give the permission to switch for forward multicast traffic to those port who request it. IGMP snooping switch protects flooded multicast traffic to all ports. IGMP snooping maintain bandwidth. IGMP snooping automatic manipulate specific group membership for static multicast group address.
6. The switch(snooping) uses intelligent multicast forwarding decisions information and forward traffic to proposed destination interfaces.
7. DHCP snooping is a DHCP security feature that provides security from non trusted DHCP message by filtering, building and maintaining a DHCP snooping binding table. DHCP snooping acts like firewall between non trusted hosts and trusted DHCP servers. DHCP snooping, network administrators can limit on who or what can access to the network.
8. At various ports, network administrators can limit the number of computers or DHCP clients that are permitted access.
9. DHCP snooping switch performs following activities:-
    1. Verify DHCP messages from non-trusted sources.
    2. Filters invalid messages.
    3. Control DHCP traffic Rate-limits from trusted and non-trusted resources.
    4. Creates and maintains the DHCP snooping binding database, which holds information of non-trusted hosts with leased IP addresses.
    5. Use the DHCP snooping binding database for valid subsequent requests from non-trusted hosts.
10. MLD snooping switch establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast database on these mappings.
    1. It works at port level and maintains network bandwidth by reducing the multicast IPv6 packets flooding.
    2. MLD snooping allows the switch to examine MLD packets and forwarding with their content.
    3. MLD snooping monitors the Layer 3 MLD traffic.

Introduction of IGMP Snooping

IGMP is used between a small number of source routers and IP clients that are located on the same logical LAN segment. This means that IGMP snooping is of most benefit in the VPLS instance where a small number of routers are attached and the majority of access circuits are Ethernet switch based.

IGMP snooping allows the intermediate device to monitor IGMP traffic. The snooping agent can stop sending multicast traffic when a leave is received. The snooping agent must also keep some state regarding general Membership Query Maximum Response Time timers in the event a LEAVE message is not issued from an IGMP

client (such as when the power cord is pulled out on an IPTV set-top box).

The snooping device is transparent, IGMP packets are read and then forwarded upstream to the multicast router. The snooping device does not participate in the IGMP host messaging and promiscuously listens to transactions between clients and routers to determine when join/leave processing is required to a downstream host.

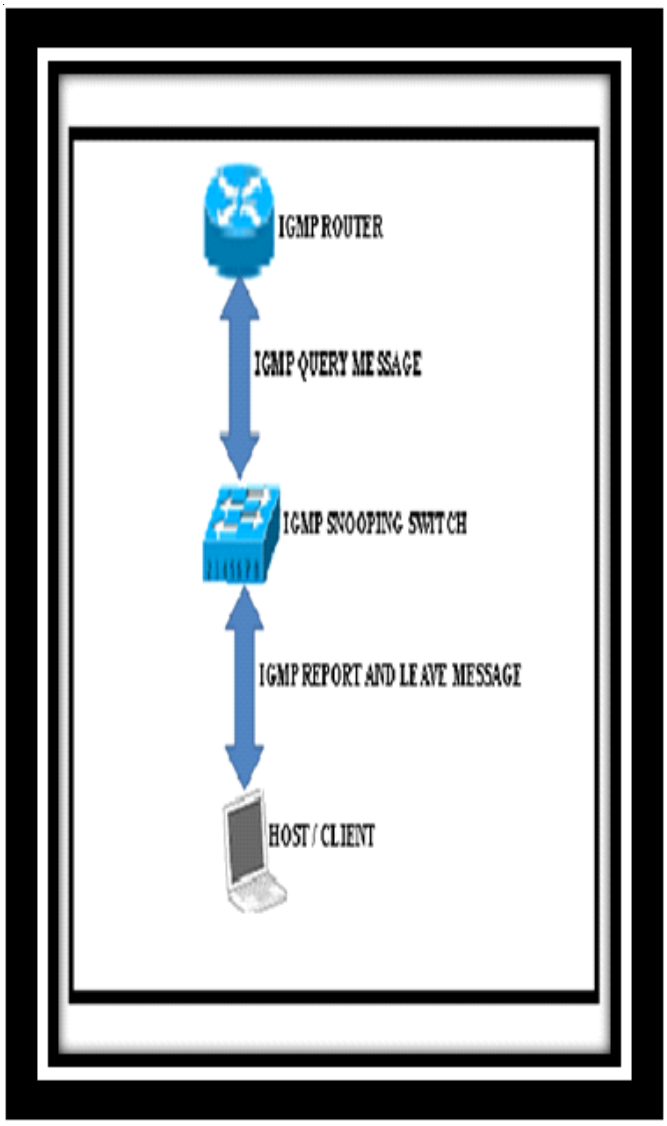

Figure: 1.1 - IGMP Snooping Process.

The snooping device will rely on one of multiple mechanisms for the actual reception of the multicast data from its upstream multicast neighbor. The router may be statically configured to flood all multicast groups downstream to the snooping device, the upstream router may only forward groups based on IGMP Membership Reports received from the IGMP hosts, or the snooping agent may invoke an IGMP client process to source its own Membership Reports that are sent to the multicast router. All IGMP packets are forwarded through the intermediate device and these packets are never modified. As a result, the upstream IGMP router has full visibility to each downstream device.

By default, the switch will only forward traffic out those ports with multicast clients, so it will not act as a simple hub. Multicast is sometimes used to advertise to clients, services available on their network through Directory Agents (DAs) or with Service Agents (SAs) using Service Location Protocol (SLP). Clients Agents (UAs) and SAs send multicast requests (224.0.1.35), to locate DAs on the network. UAs and SAs learn of DAs via periodic multicast (224.0.1.34) advertisements.

Multicast(wired and wireless lans) traffic will only be forwarded to ports identified as members of the specific multicast groups. There is no need for IGMP-joins to these addresses with SLP. When an Ethernet/IP device wants to consume multicast data, it will transmit an IGMP join message. These join messages are received by all IGMP Snooping switches and the switch "snoops" on the join messages as they pass in order to determine which ports will receive the multicast data. This restricts the multicast data to only the ports-and connected end devices-that expect and can handle the traffic.

IGMP Snooping conserves bandwidth. With IGMP Snooping, the switch learns which ports are interested in receiving multicast data, and forwards multicast data only to those ports. The multicast router sends out periodic general queries to all VLANs. All clients interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. Switch with IGMP Snooping can forward multicast messages to only the devices that request the traffic and are designed to handle it and reduce flooding.

For IGMP Snooping to work properly, one or more switches or routers in the network must provide IGMP Query support. The IGMP Querier will periodically ask each end device in the network which multicasts they wish to receive, refreshing the IGMP multicast/port associations. The IGMP Snooping Querier is used to support IGMP snooping where the multicast traffic is not routed. We can configure IGMP snooping querier to support IGMP snooping in subnets without multicast interface. IGMP Query supports multiple IGMP Queriers in the network. If there are multiple, then the IGMP Querier with the lowest IP address will act as the network Querier.

By snooping IGMP registration information, a distribution list of workstations is formed that determines which end-stations will receive packets with a specific

multicast address. Internet Group Management Protocol (IGMP) snooping regulates multicast traffic in a switched network.

The IGMP query responses, known as IGMP reports (which look very much like an IGMP join) keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the delinquent port where the end-device is located.

IGMP Snooping Working technique

IGMP snooping manages multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it.

IGMP snooping regulates multicast traffic on a VLAN to avoid flooding. When IGMP snooping is enabled, the switch intercepts IGMP packets and uses the content of the packets to build a multicast cache table. The cache table is a database of multicast groups and their corresponding member ports. The cache table is then used to regulate multicast traffic on the VLAN.

When the router receives multicast packets, it uses the cache table to selectively forward the packets only to the ports that are members of the destination multicast group. A switch running IGMP Snooping performs different actions when it receives different IGMP messages, which are:

A. When receiving a general query

- When receiving an IGMP general query, then switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:
  - If the receiving port is a router port existing in its router port list, the switch resets the aging timer of this router port.
  - If the receiving port is not a router port existing in its router port list, the switch adds it into its router port list and sets an aging timer for this router port.

B. When receiving a membership report

- A host sends an IGMP report to the multicast router in the following circumstances:
  - Upon receiving an IGMP query, a multicast group member host responds with an IGMP report.
  - When intended to join a multicast group, a host sends an IGMP report to the multicast router to announce that it is interested in the multicast information addressed to that group.
  - Upon receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group, and performs the following:
  - If no forwarding table entry exists for the reported group, the switch creates an entry, adds the port as member port to the outgoing port list, and starts a member port aging timer for that port.
  - If a forwarding table entry exists for the reported group, but the port is not included in the outgoing port list for that group, the switch adds the port as a member port to the outgoing port list, and starts a member port aging timer for that port.
  - If a forwarding table entry exists for the reported group and the port is included in the outgoing port list, which means that this port is already a member port, the switch resets the member port aging timer for that port.

C. When receiving a leave group message

- When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave group message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.
- When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave group message to the multicast router.
- When the switch hears a group-specific IGMP leave group message on a member port, it first checks whether a forwarding table entry for that group exists, and, if one exists, whether its outgoing port list contains that port.
  - If the forwarding table entry does not exist or if its outgoing port list does not contain the port, the switch discards the IGMP leave group message instead of forwarding it to any port.
  - If the forwarding table entry exists and its outgoing port list contains the port, the switch forwards the leave group message to all router ports in the VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that group address, the switch does not immediately removes the

port from the outgoing port list of the forwarding table entry for that group; instead, it resets the member port aging timer for the port.

- Upon receiving the IGMP leave group message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave group message. Upon hearing the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that multicast group, and performs the following:
  - If any IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that some host attached to the port is receiving or expecting to receive multicast data for that multicast group. The switch resets the aging timer of the member port.
  - If no IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that no hosts attached to the port are still listening to that group address: the switch removes the port from the outgoing port list of the forwarding table entry for that multicast group when the aging timer expires.

Advantage of IGMP Snooping

The IGMP snooping feature can provide the following benefits to a multicast network:

- Basic IGMP snooping reduces bandwidth consumption by reducing multicast traffic that would otherwise flood an entire VPLS bridge domain. IGMP snooping can provide security between bridge domains by filtering the IGMP reports received from hosts on one bridge port and preventing leakage towards the hosts on other bridge ports.
- IGMP snooping can reduce the traffic impact on upstream IP multicast routers by suppressing IGMP membership reports (IGMPv2) or by acting as an IGMP proxy reporter (IGMPv3) to the upstream IP multicast router. Hosts only receive MC traffic that they request. "Fast-leave" functionality - stop sending MC group as soon as switch hears a "leave" on an interface.
- IGMP Snooping Report suppression - prevents first-hop router from being flooded with IGMP reports for the same group.
- IGMP Snooping provide Powerful tools for Sophisticated, application-aware classification engine, per-client scheduling and prioritization for WLANs provides precision bandwidth management, traffic shaping and service level agreements for video, voice and data.
- IGMP Snooping give superior Performance for Eliminates jitter and delay for video and voice, providing quality of service and outstanding user experience. IGMP Snooping provides Guaranteed multicast streaming for the only proven QoS system for IPTV, Smart Cast converts multicast traffic to unicast, delivering video traffic to each subscriber at the highest data rate that the client is capable of supporting.
- IGMP Snooping provides Optimal utilization for Airtime fairness which provides efficient use of the available spectrum, resulting in greater network capacity in high-density and diverse client environments. IGMP Snooping increased efficiency and capacity in band steering directs dual band clients to the less congested 5 GHz spectrum, while load balancing directs clients to less congested APs, distributing client load across all available channels and APs.
- IGMP Snooping is Easy to use in smart heuristic-based classification automatically provisions QoS services. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (IGMP client). A switch that does not IGMP snoop will, by default, 'flood' multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent).
- IGMP snooping takes place internally on switches and is not a protocol feature.

Configuration for IGMP Snooping with automatic indexing

Table: 1.1- The default configuration values for IGMP snooping queries.

Steps	Features	Default value
1	The IGMP snooping queries in a VLAN	Disable
2	IGMP Snooping	Enabled globally and per VLAN
3	VLAN interface dynamically accesses a multicast router	PIM-DVMRP

4	Static connection to a multicast router	Enable
5	Configuring a Static Connection to a Multicast Receiver	Not configure
6	Configuring a Multicast Router Port Statically	Not configured
7	Configuring a Host Statically to Join a Group	Not configured
8	Configuring the IGMP Snooping Query Interval	Not configured
9	IGMP Fast-Leave Processing	Disable
10	IGMP Immediate Leave	Disable
11	Configuring the IGMP Leave Timer	The default is 1000 seconds
12	Configuring Source Specific Multicast (SSM) Safe Reporting	Disabled; deprecated in Release 12.2(18) SXE and later releases
13	Configuring IGMPv3 Explicit Host Tracking	Disable
14	Disabling IGMP Report Suppression	Enable
15	Controlling a TCN Event before the Multicast Flooding Time	2
16	Recovering from Flood Mode	Not configured
17	Multicast Flooding During a TCN Event	enabled on an interface.
18	Configuring the IGMP Snooping Querier	Not configured
19	IGMP Report Suppression	Enable
20	IGMP Snooping END	
21	Display igmp snooping	

Table: 1.2- Display IGMP Snooping Indexing

Sno	Options
I	According vlan-id.
II	According interface-id.
III	According IP- Address.
IV	According MAC- Address.
V	According QOS.
VI	According ports.
VII	According source / group.
VIII	According reporter.
IX	According uptime.
X	According last join.
XI	According leave time.
XII	According datetime.
XIII	According pim mode.
XIV	According Message type / size.

Disadvantage of IGMP Snooping

IGMP Snooping works in networks but this cannot protect completely. It cannot protect from various attacks which are:-

- IGMP Snooping not protected from server spoofing attacks.
- IGMP Snooping cannot differentiate in trusted and non trusted clients.
- IGMP Snooping not provides security against address exhaustion attacks.
- IGMP Snooping not protect IP address Hijacking.
- IGMP Snooping not prevents from rough server or unauthorized server attacks.
- IGMP Snooping not prevent from starvation attacks.
- IGMP Snooping not protect in IP / MAC spoofing attacks.

CONCLUSION

IGMP snooping is important technique, it is use for analyzes all IGMP packets between host and multicast router in network and prevent host on a local network from receiving traffic for multicast group which have not explicitly joined. IGMP snooping controlling the flooding of multicast traffic by dynamic configuration methods and forward this traffic to only those interface which associated with multicast devices and update with multicast group membership on port by port basis.

IGMP snooping works between host and router and record multicast groups and member ports and also prevents a duplicate report which is send to multicast device by report suppression. IGMP snooping querier support snooping where the multicast traffic is not routed and also updates periodically status of attached devices.

Bibliography

Websites

1. http://en.wikipedia.org.

2. http://www.cisco.com
3. http://www.h3c.com
4. http://www.juniper.net
5. http://www.etutorials.org
6. http://www.h3c.com.

BOOKS

1. **CCNP Security Secure -Quick Reference by** Andrew Mason., Cisco Press , 2001
2. **IGMP Snooping by .** Lambert M Surhone, Mariam T Tennoe, Susan F Henssonow, VDM Verlag Dr. Mueller AG & Co. Kg, -2010
3. **Network security architectures.** By Sean Convery, Cisco Press, - 2004
4. **Cisco LAN Switching Configuration Handbook.** By Steve McQuerry, David Jansen, Dave Hucaby, Cisco Press, -2009
5. **Fundamentals of Network Security** By Eric Maiwald, McGraw-Hill Professional, -2003

Research papers

1. **"Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches"** Author:- M. Christensen ,Thrane & Thrane, F. Solensky, Calix. May 2006
2. **"Research on IGMP and its Implementation for Switch Management"** Author:- Sheng Lu., Advanced Materials Research -2011 (Volumes 219 - 220)