Application of ACL Technology in the Security of IP DSLAM Network

Liu Li, Wei Zhi
(Fiberhome Technology, Wuhan Institute of Posts and Telecommunications
E-mail: liliu@fiberhome.com.cn)

Abstract:

In the processing of extending scale of network and enlarging flock of consumers, the security of network plays an extremely important role. This paper presents an access control technology to enhance the management of information security, and analyses the detailed principle of the key technology—multi-layer flow classification.

Key words:

Network security, Access Control Technology, Multi-layer Flow Classification

1. Foreword

In the same period of broadband access network's gradual transformation to IP, a large-scale communication network entirely based on IP has formed. Coming in for the progress of technology and the driving of competition, IP network wants to bear the weight of new more operations, so the network security problem is raised to a no higher height.

In order to organize and manage information in each departmental of company with an unitive method, staff and exterior client server all have possibilities to contact the kinds of information. So some sensitive communication or business secret must be carried under the security control. The impact after taking this measure is that only those consumers invested with privilege can search the confidential information.

2. The application background of ACL technology

IPDSLAM (Internet Protocol Digital Subscriber Line Access Multiplexer), because of providing high density with low ullage broadband link、flexible uplink port and downlink network ability, it gets unshakable station. It uses today's fastest DSL technology to support cutting-edge, high-value applications, like video-on-demand, broadcast T.V. and super-high-speed Internet access.

With broadband access network scale's grandly increasing, the operation mostly with IP and network environment are on the road to maturation, IPDSLAM already becomes construct mode of mainstream broadband.

Consumer can deliver these bandwidth-intensive services cost-effectively over existing copper wiring, because very high-speed DSL (VDSL) transports data at rates up to 70 Mbps downstream and 40 Mbps upstream. IP DSLAM includes the key features the user need to streamline delivery of sophisticated services for both business and residential subscribers. It provides a rate adaptive function to optimize transmission rates; link aggregation to increase available bandwidth; tagged VLAN capabilities that enable DSL wholesaling and Internet Group Management Protocol (IGMP) snooping that helps users control traffic for streaming media, video conferencing and other data-intensive services. IP DSLAM gives users a highly cost-effective way to achieve the transport speeds required for high-margin broadband applications, like streaming media and interactive gaming.

ACL technology applied to IPDSLAM system is an effective method to solve the problem of network security, and it can take distinct impact.

3. Access Control List’s presentation

ACL (Access Control List) is a method, which authorizes or constrains access privilege and range through validating consumer’s identity and limiting network flow.

The primary purpose of an access control system is to regulate who can go where, and when they can go there. The who is determined by the people enrolled into the access control system (usually by typing in their name and other relevant information) and who are provided with a security access control card. These are the authorized users of the system. The where is determined by the doors and gates (sometimes both are referred to as “portals”) at which the access control card readers are installed. There are two aspects to the when of access control. Where and when a user is allowed to go is called the user's access privilege. The definition of access privileges will vary slightly from system to system, but they all involve a way to associate a portal with an authorized access time. Although many systems offer the ability to define custom access privileges on a per-user basis, that approach is too cumbersome and time-consuming for managing the privileges for the majority of users in a large system.

Most systems provide access levels (an access level is a named list of portals and access days and times) for groups of people who have the same access requirements, to facilitate plain-English management of access details. For example, an access level named Engineering could define the access privileges for the airport's Engineering personnel. Using self-explanatory access level names makes it easy to assign access privileges to users without having to review the details every time a new user is enrolled. Furthermore, access levels provide a way to easily apply security policies. System expansion is facilitated by the use of access levels, since it is easier to add a new door to a group of access levels than to add the door separately to each individual's record.

Often a set of access times (days of the week, and hours of the day) can be defined as a named Schedule (sometimes called a Time Zone), so that it is not necessary to repeatedly type in the time details for each door or access level. The ability to name schedules, such as weekdays, seven days a week, or midnight shift makes it easier to create and manage access levels. Access groups are provided to further assist in the management of access. Access levels can be named for the physical locations or areas to which they provide access, and access level groups can be named for the categories of users.

Using access control service, we can constrain visitation to the key resource, prevent the incursion from non-legal consumers and the destroy because of unmerited operation by legal consumer. This technology takes on non-substitutable role in the network security system.

4. The key technology of ACL——Multi-layer Flow Classification

4.1 The definition and configuration of the control access function system

In the integrity system of ACL, the control access function system includes:

(1) Subject: the initiative side of sending access operation or storing request. Usually it refers to the consumers or the process of consumers.

(2) Object: the transferred process or the data access which will be stored.

(3) Security access rule: it is used to confirm that a subject has access authorization to some objects or not.

Multi-layer flow classification may be triggered to override Class-Of-Service and routing/switching decisions for a given packet with sophisticated criteria and also to provide extended filtering capabilities. It may be used as an extension to the IPX routing services, and also as an extension to the regular Layer 2 switching process.

4.2 How to realize advancing CoS with Multi-layer Flow Classification technology

CoS (Class-of-Service) is the standard recognized by the most people. For a given packet with sophisticated criteria, multi-layer flow classification may be triggered to override Class-Of-Service and routing or switching decisions. It also to provide extended filtering capabilities. This function may be used as an extension to the IPv4/IPX routing services, and, independently, as an extension to the regular Layer 2 switching process.

A basic classification can also be performed based on the IPv4 Protocol field or TCP/UDP port numbers.

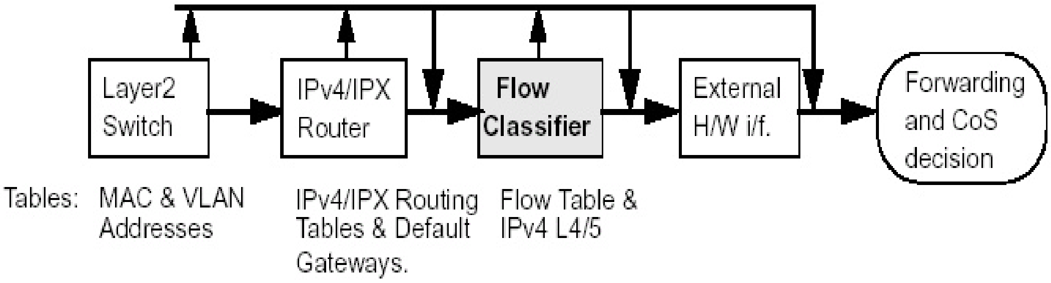

Figure: Multi-layer Flow Classification Unit

There are four master flow classification functions that support multi-protocol classification. Each flow classification function is defined by a flow type. Of the four flow types; one can be used for IPv4 and one for IPX.

Each Non-multicast IP Address can belong to one of 32 address groups referred to as “Access Groups”. An Access Group may be an IP end-station, server, group of servers, network, group of networks etc.

5. The improvement with Multi-layer Flow Classification

After adopting this function, a policy can be applied per flow, where each flow can be dropped, passed to the CPU, passed for further treatment by External Hardware, or only classified to the transmission queue. This can be used for implementing application-based access control list.

The classification procedure determines the Class-Of-Service of a given packet by setting the following three parameters: The packet’s transmit priority queue, the discard ability, and the packet’s VLAN priority tag for ISSLL implementation.

An input-rate control can be applied per flow using the token bucket mechanism, and an oversubscribing flow can be dropped or marked with high drop precedence.

The classification may also modify the target port and device that were set by the Layer 3 routing or Layer 2 switching for “Layer 4 switching”, for load balancing over link aggregate, or for switching proprietary protocols.

6. Conclusion

In conclusion, for improving the network security and authorizing consumers visitation, using ACL technology and its key principle, multi-layer flow classification is an effective method. How to make the security technology applied properly without affecting the network performance is a research item that is considered of having great signification and possesses most expansive foreground to develop.

参考文献

1．Ray Bernard. Controlled Access. Access Control & Security Systems, 2003

2．Converged Voice/Data Network Switch Processors. Galileo Technology,2002

3．V-16^{TM} IP DSLAM Product Description. Lucent Technologies, 2003

4．**李晓林**. **一种新型的** INTRANET **信息安全控制**. **计算机工程与应用，**2002

5．**宾晓华**. **企业网络安全问题研究**. **计算机工程与应用，**2002

6．Carey Adams. Single Card Access, Decentralized Control at Georgia Tech. Access Control & Security Systems, 2001