A FRAMEWORK FOR POLICY-BASED SLA MANAGEMENT OVER WIRELESS LAN

Noh-sam Park, Gil-haeng Lee
Electronics and Telecommunications Research Institute

Keywords: Service Level Agreement, SLA, SLM, QoS.

Abstract: With the evolution of wireless networks, the wireless community has been increasingly looking for a framework that can provide policy-based SLA management. In this paper we first construct such a framework and then describe how SLA-based control can be used to achieve QoS in wireless environment. We provide a common generic framework capable of components to interwork via XML. The proposed framework offers effective WLAN QoS control and management using client-side agent.

1 INTRODUCTION

In an environment of fast changing technologies and uncertain business tendencies, network operators, constructors, and organizations face new challenges to keep up with the increasing needs of ubiquitous network. This is a major driver for the technological development of wireless networks.

A service level agreement (SLA) is a formal contract between a service provider and a subscriber that contains detailed technical specifications called service level specifications (SLSs). An SLS is a set of parameters and their values that together define the service offered to a traffic stream in a network(F. De Turck, 2001).

An SLA can be defined and used in the context of any industry and is used to specify what the customer could expect from the provider, the obligations of the customer as well as the provider, performance, availability, and security objectives of the service, as well as the procedures to be followed to ensure compliance with the SLA.

Some work has been done in defining SLAs for traditional IP networks(Verma, 2004). Because wireless LAN(WLAN) technologies belong to an emerging domain, until now, no SLAs have been defined that are adapted to the specific needs of WLAN.

This work focuses on defining these SLAs specifically adapted to the relationship between W LAN operators and their diverse clients. Moreover, we propose a policy-based SLA management framework that provides effective QoS control and management.

The remainder of this paper is structured as follows. Section 2 will discuss related works on SLA management over other networks. After describing the metrics related WLAN in section 3, we will explain a framework of SLA Management system for WLAN environment in section 4. Finally we'll summarize our work and sum up the conclusions from this study

2 SLA MANGEMENT IN NETWORK SERVICES

The importance of SLA has been recognized and widely accepted by ASP's, ISP's, etc. In particular, this section reviews features of various SLA management systems for network services.

The work for service level agreement in optical networks has been done(Fawaz, W, 2004). It proposes a service level agreement applied to the optical domain (O-SLA), which is expected to be the near- and long-term network technology thanks, among other things, to the great bandwidth capacity offered by optical devices. After an exposition of the rationale behind an optical SLA, parameters that could be included in this O-SLA, as well as their values for four classes of services, are proposed.

Park N. and Lee G. (2005).
A FRAMEWORK FOR POLICY-BASED SLA MANAGEMENT OVER WIRELESS LAN.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 173-176
DOI: 10.5220/0001409401730176

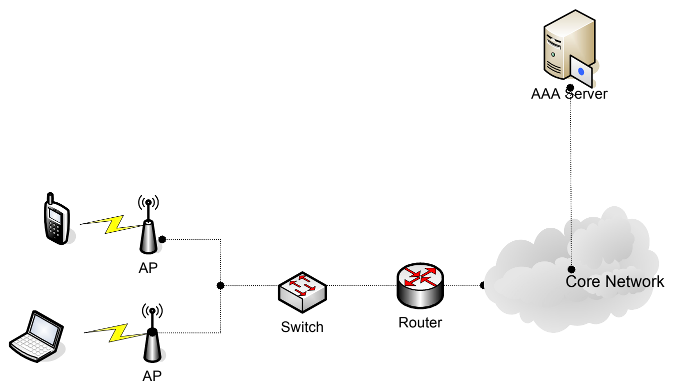

Figure 1: Wireless LAN

In traffic and performance parameters for O-SLS, it describes the followings.

- Connection setup time
- Service availability and resilience
- Routing constraints(Stability, Route Differentiation, Confidentiality, Distance, Classes of Service)
- Service performance guarantees
- Traffic conformance and excess treatment

Furthermore, some values for O-SLS parameters are proposed for four classes of service (from platinum to bronze, excluding best effort traffic for which no guarantee at all is provided).

Different client (wavelength or subwavelength) and service types (from leased wavelength to bandwidth on demand) are distinguished when necessary.

In (Verma, 2004), it provides an overview of service level agreements in IP networks. It looks at the typical components of an SLA and identifies three common approaches that are used to satisfy SLAs in IP networks. It describes the components of SLAs :

- A description of the nature of service to be provided.
- The expected performance level of the service, specifically its reliability and responsiveness.
- The procedure for reporting problems with the service.
- The time frame for response and problem resolution.
- The process for monitoring and reporting the service.
- The consequences for the service provider not meeting its obligations.
- Escape clauses and constraints.

Three common approaches are used to support and manage SLAs. The first approach takes the model of an insurance company toward monitoring and supporting SLAs. The second approach uses configuration and provisioning techniques to support SLAs within the network. The third approach takes a more dynamic and adaptive approach toward supporting SLAs.

The implications of using the approaches in the context of a network service provider, a hosting service provider, and an enterprise are examined. While most providers currently offer a static insurance approach toward supporting SLAs, the schemes that can lead to more dynamic approaches are identified.

3 SLA ISSUES IN WIRELESS LAN

Access to data services via wireless LANs at private and public hot spot sites is becoming commonplace(Acharya, 2004). Wireless access solutions based on the IEEE 802.11 family of standards are mushrooming in many different places where people congregate, like airports, hotels, cafés, train stations, and parks. These public congregation areas constitute connectivity islands, or *hot spots*, where broadband access services can be provided wirelessly to one's personal devices, such as notebook computers and PDAs.

As usual, during the communication session at a hot spot area, the following phases are experienced:

- *Personal device configuration* : During this phase, user devices are properly configured and permitted access to the hot spot site's intranet.
- *User Authentication* : During this phase, users provide identification credentials to the system. These could be provided explicitly, where a user explicitly provides personal information, or implicitly, where a pointer to a stored log-on profile is provided by the users or their devices.

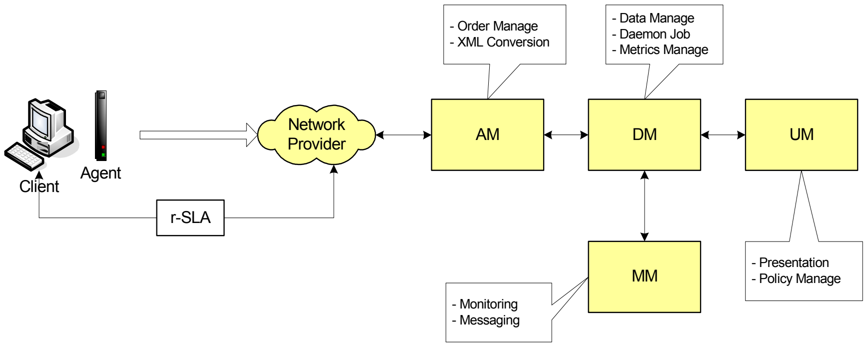

Figure 2: Framework of SLMS

- *Service access control* : During this phase, the intelligence configures the hot spot site's intranet to allow users to access only services within the service tier they have selected.
- *Session management* : This is a supervisory activity that keeps track of user sessions including their service tier selections, the duration of accessing services at a selected tier, or traffic statistics.

We derive the SLA metrics related WLAN from its inherent properties. In this environment, typical clauses related to performance and availability may look like the following.

- The average delay measured monthly between the hot spot and router in core network should be less than 200 ms.
- The customer will not have unscheduled connectivity disruption within hot spots exceeding 5 min.
- The connection setup time, representing the time between service ordering and service availability, should be less than 30 seconds.

4 FRAMEWORK FOR SLM OVER WLAN

The framework for policy-based SLA management(SLMS) supports the QoS control in WLAN environment. The framework incorporates two key ideas: a generalized monitoring concept, and a contract negotiation and translation feature for all the components. It includes automation of r-SLAs(retail SLAs), not w-SLAs(wholesale SLAs).

4.1 Components

SLMS framework proposes the architecture that partitions system functionalities into five major components : an access manager, a data manager, a monitoring manager, a user interface manager, and a Agent(Fig. 2).

Access Manager (AM) : The AM is the entity that receives the information related service opening, trouble and performance. It is responsible for translating the information into XML format, pushing the translated XML document into the message queue.

Data Manager (DM) : The DM reads the XML data from the message queue, classifies the data according to the SLA metrics. As the DM manages the information in the database, it can response to the UM the retrieve and save the SLA related data.

Monitoring Manager (MM): The MM plays the important role of monitoring the violation of SLA metrics. Periodically it monitors whether QoS violates the SLAs. If the MM detects the violation, it sends the violation information through the message queue.

User interface Manager (UM): The UM interacts with the operators, and provides the variety of data including the alert messages. Operators can configure the policy of SLM such as the execution of monitoring or not.

Agent: The client-side agent collects the performance data by polling the access router at the core network periodically. And it records the connection setup time per session. The agent sends those information to the AM.

The combined role of these components is to efficiently manage SLA of the service, present the QoS information, and appropriately refund if the violation of SLA happens.

4.2 Prevention of the SLA Violation

Monitoring is the core function of our framework to prevent the violation of SLA. We developed the monitoring function reacting not only when an SLA is violated, but also before imminent SLA violations. Our system has the monitoring component which checks the threshold at first, and compares the metrics value secondly. The threshold is the value which can be alerted to the operator by sending the 'warning'. If the operator receives the warning message from the system, he/she reviews the details, and can take an action to prevent the violation of SLA.

The MM has the following monitoring functions : service opening, trouble, and performance monitoring. At the system initiation stage, the MM creates three threads in order to monitor the categorized metrics.

At the defined thread invoke time, the MM periodically creates threads. Threads retrieve the monitored data, threshold and metric. Firstly, the MM thread compares the data with the threshold. If the current value is greater than the threshold, the 'warning' message is sent to the AM via XML format. The MM thread will detect the violation of SLA by comparing the issued time with metric value. If the violation event occurs, the 'violation' message will be sent, and the violation details is recorded in the database through the DM. Finally, the threads are disposed after execution.

Policy-based monitoring can be accomplished by configuring the various preferences. The interval of monitoring can be changed by using the UM. If the operator changes the monitoring interval, the UM sends the message to the MM. The MM receives the event, and changes the thread invoke time. Furthermore, the operator can have the metrics monitored or not. Using the UM, the operator can configure whether the metrics are monitored or not. If the metric is set not to be monitored, the MM will not execute the monitoring function. But if the history of warning and violation is recorded in the database, and can be retrieved via the UM.

5 CONCLUSIONS

We propose a form of architecture for an SLA Management System using web service. We first explore the SLA-related works in various network environments. As describing the characteristics of WLAN, we issued the metrics related WLAN. A framework for SLM over WLAN are introduced with detailed description of its components. Our system has the capability to manage the SLA from the service opening to the service termination. By using the client-side agent which collects the network performance information, we can easily manage the SLA, and control the QoS.

According to the implications of the research, future work has been conducted to interwork Operation Supporting Systems (OSSs) such as the refund system and NMS.

REFERENCES

F. De Turck et al., 2001. *Design and Implementation of a Generic Connection Management and Service Level Agreement Monitoring Platform Supporting the Virtual Private Network Service*, Integrated Network Management Proceedings.

Verma, D.C., 2004. *Service Level Agreements on IP Networks*, Internet Computing, IEEE.

Fawaz, W., Daheb, B., Audouin, O., Du-Pond, M., Pujolle, G., 2004. *Service level agreement and provisioning in optical networks*, Communications Magazine, IEEE

K. Trzec, B. Mikac, 2004. *On Agent-based Service Level Agreement Management in Optical Internet*, MELECON, IEEE.

R. Chakravorty, I. Pratt, J. Crowcroft, 2003. *A framework for dynamic SLA-based QoS control for UMTS*, Wireless Communications, IEEE.

M. Buco, Rong Chang, L. Luan, C. Ward, J. Wolf, P. Yu, 2003. *Managing eBusiness on demand SLA contracts in business terms using the cross-SLA execution manager SAM*, ISADS.

M. D'Arienzo, M. Esposito, S.P. Romano, G. Ventre, 2003. *Automatic SLA Management in SLA-aware architecture, Telecommunications*, 2003 (ICT 2003).

G. Cortese, R. Fiutem, P. Cremonese, S. D'antonio, M. Esposito, S.P. Romano, A. Diaconescu, 2003. *CADENUS: creation and deployment of end-user services in premium IP networks*, Communications Magazine, IEEE.

Acharya, A., Bisdikian, C., Misra, A., Young-Bae Ko., 2004. airConn: *A framework for tiered services in public wireless LAN hot spots*, Communications Magazine, IEEE