Ibrahim Khalil

Dynamic Service Provisioning in IP Networks

Doctoral Dissertation
Supervisor: Prof. Dr. Torsten Braun
University of Berne

Abstract

There are two key issues that businesses consider when evaluating the use of Internet for any application: Quality of Service (QoS) and Security. Fortunately, solutions exist to address both the issues. A widely used approach to tackle the security problem is a Virtual Private Network (VPN). An IP VPN is a private network on a public network infrastructure like Internet and uses tunneling technology to make private IP networks secured and public IP-compatible. By using encryption data passed through the VPN tunnel can be encrypted and protected. As a solution to QoS problem Internet Engineering Task force (IETF) has recently developed Differentiated Services (DiffServ) technology. With DiffServ, traffic entering a network is classified and given special treatment making it possible to create Virtual Leased Line (VLL) between two enterprise networks. A marriage of QoS and VPN is particularly fruitful solution for corporate communication is that of a QoS enabled IP VPN (QoS-VPN). The abilities of QoS enabled VPNs to emulate a private wide area network using IP facilities and guarantee bandwidth and latency have recently generated tremendous interest in its wide spread deployment to replace the expensive dedicated private leased lines.

However, the complexities introduced by VPNs and the requirement to provide QoS have made the job of the ISPs and systems administrators extremely difficult, and as today's network infrastructure continues to grow, the ability to manage increasing complexity is a crucial factor for VPN solutions. But, at the same time, this also opens the possibility for ISPs to sell VPN services to mostly corporate end users. Because of the complexities enterprise customers having several sites and large number of devices are willing to outsource their VPNs and other network service management to ISPs. There are economic reasons too. Most customers want the provider to assume the network management headaches, and in fact, many businesses do not have IT staff already trained in high-end-security/VPN technology. As providers take responsibilities of VPNs and other network resource management and gain economies of scale, they are facing new challenges. This thesis identifies and addresses these challenges and proposes novel solutions to ease network management for ISPs or large enterprises. These solutions include automated QoS- VPN service Activation, Simplified VPN/QoS Management in Mutivendor Environment and multi-ISP scenarios, service assurance and billing etc.

In the dissertation we proposed a policy-based Service Broker (SB) architecture and provided its implementation that uses QoS and security policy templates to generate device specific QoS-VPN configurations and automate service activation process by delivering generated configurations using agents called configuration daemons. The Service Broker (SB) system allows not only network administrators but also corporate customers to customize and activate QoS-VPNs dynamically on the fly via a web-based front end. We have also extended the implementation to create VLLs over multiple ISP domains. Corporate customers having SLA with ISPs specify security policies and bandwidth demand via the web interface. Such bandwidth demand could be a single Quantitative value (eg. 1 Mbps, 2 Mbps or 3 Mbps etc.) or range of values like 1-2 Mbps, 0.5-1 Mbps ect. This is

important because some customers will be unable or unwilling to predict the load between VPN endpoints. We realized this requirement by a novel mechanism called range-based SLA. It is used to logically partition the capacity at the edges to various classes (or groups) of VPN connections and manage them efficiently to allow resource sharing among the groups in a dynamic and fair manner. The range-based SLA is further exploited in a new scheme called virtual core provisioning to have higher multiplexing gain, and eliminate the need to provision the physical core devices in real-time. The scalable and flexible virtual core provisioning method requires only a capacity inventory of interior devices in an ISP network to be updated based on VPN connection acceptance, termination or modification at the edges.

We developed an automated device configuration audit technique to be applied in a large scale network environment that is considered to be an extremely useful feature by network managers, but rarely addressed by researchers. Intelligent audit agents can be periodically sent to the network devices to check the consistency of network device configuration, and also automatically fix the problem when one is found. Thus audit management ensures that the configuration state in the policy repository is equivalent to actual device state.