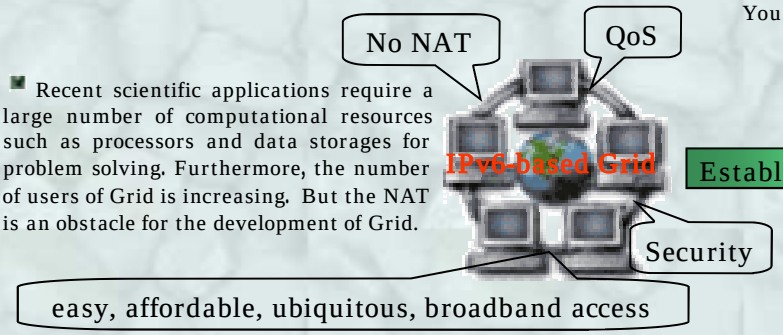
Grid needs IPv6

Grid is the most promising technology that may be an infrastructure for both business and science. This kind of infrastructure needs to be established at the world-wide scale. The following facts are part of the reasons why IPv6 is required by the Grid.

- Virtual community and virtual laboratory both which are formed across the borders of institutions and organizations by the Grid, often demands on a robust security infrastructure.

- Recent scientific applications require a large number of computational resources such as processors and data storages for problem solving. Furthermore, the number of users of Grid is increasing. But the NAT is an obstacle for the development of Grid.

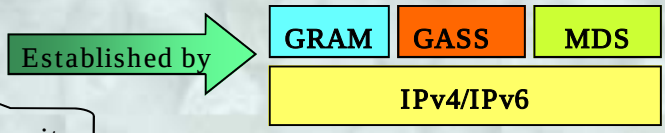


Therefore the natural scene for the future of Grid is in IPv6.

Porting Globus to IPv6 enabled

For the reason, we have ported Globus so that it can run on IPv6 network. This initial work of porting was performed for Globus 1.1.3 running on FreeBSD. And now we have ported Globus2.2.3 to IPv6 enabled which has been test on Redhat7.3. The IPv6 enabled Globus2.2.3 is dual stack for IPv4/IPv6 and is available for some components such as GRAM, GASS, and MDS.

You can download it from:http://www.biogrid.jp



IPv6 enabled Globus2.2.3

IPsec for Grid security

IPsec is the standard suite of protocols for network layer confidentiality and authentication of Internet traffic. For many applications, security at the network layer has a number of advantages over security provided elsewhere in the protocol stack. The detail of network semantics are usually hidden from applications, which therefore automatically and transparently take advantage of whatever network-layer security services their environment provides. More importantly, IPSec offers a remarkable flexibility: we can creatively use cryptographic algorithm, port and protocol to establish IPSec-protected connections. This feature of flexibility in configuration is suitable and useful for building secure Grid environment on the top of network where a diversity of security policies exists. For example, we can apply a distinct security policy to TCP/UDP port.
Thus, we combine GSI and IPSec to realize a secure Grid environment.

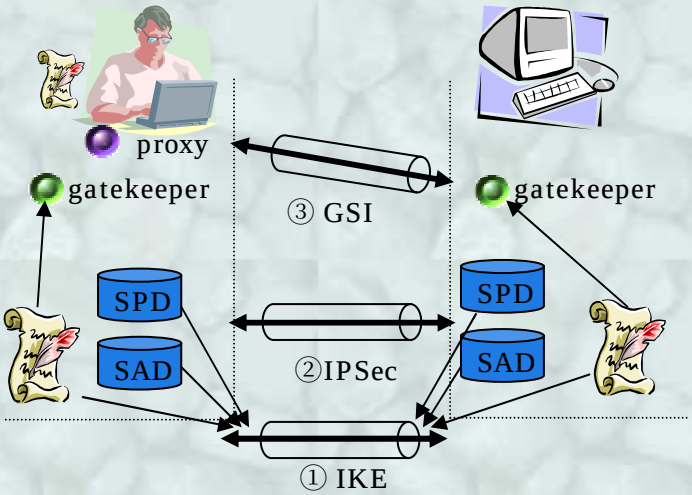
Integration of IPSec facility to GSI

For the simultaneous use of IPSec and GSI, we consider the following two issues should to be tackled.

- One is non-invasiveness to the existent Grid architecture from the viewpoint of user. Globus has prevailed as de facto standard of Grid implementation and many Grid projects have already adopted Globus as a building block to build their own application systems on the Grid. Therefore the specification, such as the number of arguments of the APIs provided by Globus, must not be changed for the integration of IPSec.

- Another is selectivity for balancing the trade-off demand between high-performance and confidentiality. In the Grid, a variety of data is supposed to be treated. Each type of data has a demand on confidentiality. Furthermore, the amount of data is ranged from a few kilobytes to more than petabytes. This situation produces the demand on switching the strength of confidentiality level provided by IPSec according to criteria such as data amount and data importance. Thus we consider the mechanism allowing user to balance two demands: high-performance and confidentiality.

Architecture of secure Grid environment



Secure Grid mechanism

① Firstly, a pair of IKE entities user the certificates issued by Globus CA for gatekeeper to authenticate each other. After that, IKE negotiate SA between IPSec entities based the information of SPD and SAD.

② Secondly, a pair of IPSec entities are mutually authenticated via the IKE connection and then establish a IPSec-protected connection.

③ Finally, the user proxy and the gatekeeper on the remote computer trust each other using GSI authentication , so that the user can execute a job on the remote computer.