

Title: ESnet On-Demand Secure Circuits and Advance
Reservation System (OSCARS)
PI Name: Chin Guok
PI Institution: Lawrence Berkeley National Lab

Project Website: www.es.net/OSCARS

Abstract:

With the advent of service sensitive applications (such as remote controlled experiments, time constrained massive data transfers, video-conferencing, etc.), it has become apparent that there is a need to augment the services present in today's ESnet infrastructure.

Two DOE Office of Science workshops in the past two years have clearly identified both science discipline driven network requirements and a roadmap for meeting these requirements. This project begins to address one element of the roadmap: dynamically provisioned, QoS paths.

The focus of the ESnet On-Demand Secure Circuits and Advance Reservation System (OSCARS) is to develop and deploy a prototype service that enables on-demand provisioning of guaranteed bandwidth secure circuits within ESnet. OSCARS will leverage existing (or in development) products, services, and code (both from the industry and academia) to accomplish its goals. OSCARS will utilize the existing DOEGrids certificate infrastructure and modify Virtual Organization Membership Services (VOMS) software to implement its authentication and authorization schemes. The management and operation of end-to-end circuits (using Label Switched Paths (LSPs)) within the network will be supported using Multi-Protocol Label Switching (MPLS) and Resource Reservation Protocol (RSVP). Quality of Service (QoS) will be used to provide bandwidth guarantees.

The project objective is to develop and deploy an intra-domain service that can be used by ESnet attached sites, but that will eventually be able to be used by a bandwidth broker to set up inter-domain QoS paths.

Interoperability with emerging standards, in particular the OASIS's Web Services Resource Framework (WS-RF) and the Global Grid Forum's Open Grid Services Architecture (OGSA), will be a focal point in the implementation of this project.

The research aspects of this project are the investigation of how all of the various elements of the OSCARS service can properly interact with deployed network tools, and how the overall service can co-exist with the production network.

Project Description

The intent of OSCARS is to create a service for dynamic QoS path establishment that is simple for users to use. The only task required of a user is to make a bandwidth reservation. The user does not have to configure an alternate routing path, nor mark the packets in any way. All necessary mechanisms needed to provide the user with a guaranteed bandwidth path are coordinated by a Reservation Manager (RM) and managed by the routers in the network.

QoS, MPLS, and RSVP

The implementation of an assured bandwidth path consists of two components: 1) The end-to-end path (or circuit), and 2) the guarantee of bandwidth on the path. MPLS and RSVP will allow us to create the circuit using an LSP, and QoS will guarantee the bandwidth.

Reservation Manager (RM)

The Reservation Manager (RM) will be comprised of three components, the Authentication, Authorization, and Auditing Subsystem (AAAS), Bandwidth Scheduler Subsystem (BSS), and the Path Setup Subsystem (PSS). The RM will have an architecture that is consistent with the WS-RF model of a service, even if it does not initially implement all of the WS-RF conventions. It will define a language independent standard interface using the Web Service Description Language (WSDL). The system state is managed by the RM and is invoked through a standard service interface using the Simple Object Access Protocol (SOAP) protocol. This will facilitate the option for other applications, irrespective of programming languages (including middleware) using SOAP to communicate directly with the RM, and will allow for more full integration with WS-RF as implementations mature.

Authentication, Authorization, and Auditing Subsystem (AAAS)

The AAAS will be responsible for authenticating the requester and validating the authorization of the requests for bandwidth usage. The AAAS will receive signed SOAP messages (either from the WBUI or an equivalent application) with the reservation information and an authenticated identifier (such as a DOEGrids certificate). This will be done through a standard published interface using WSDL. Authorization and auditing (with further investigation) may potentially leverage off a customized Virtual Organization Membership Service (VOMS). Auditing information generated from usage records will be used in the future for accounting and allocation management.

Bandwidth Scheduler Subsystem (BSS)

The BSS will be responsible for tracking the reservations of the various links within ESnet involved in the end-to-end bandwidth guaranteed paths. The BSS must be able to say whether a reservation request is compatible with the QoS service offering combined with the current state of the network. (I.e., is there sufficient QoS capacity throughout the life of the requested reservation to accept the reservation?) In order to effectively make the reservations, it is essential that the BSS is aware of the state of the network (present and future). To accomplish this, the BSS will need to interact with existing production tools that monitor and coordinate changes in the network.

Path Setup Subsystem (PSS)

The PSS is responsible for setting up and tearing down the on-demand bandwidth paths. This is accomplished by making the necessary configuration changes in the routers to create or destroy a Label Switched Path (LSP) at the times dictated by the BSS. The authentication and authorization method for the PSS is internal to the ESnet network and will be specific to the router platform (currently Juniper or Cisco) being configured, and is therefore distinct from the AAA used by the BSS.

Deployment and User Access

OSCARS will be deployed as an ESnet-wide service allowing users to reserve guaranteed bandwidth circuits between ESnet border routers. Users will make reservation requests to the RM via a Web-Based User Interface (WBUI). Communication between the WBUI and the RM will be authenticated and secured initially using HTTPS, although as WS-RF matures it is likely that WS-Secure Conversation will be used for this purpose. Once a reservation has been made, all further action required to manage (setup, police, and teardown) the guaranteed bandwidth circuit (LSP) will be transparent to the user. Packets sent by the user's system will be automatically filtered out by the ESnet ingress border router and injected into the LSP to be switched towards the ESnet egress border router. The ESnet egress border router will then extract the packet from the LSP and route it to its destination.