Role-Based Access Control
// Feature Brief

Unified Visibility Fabric™ Architecture

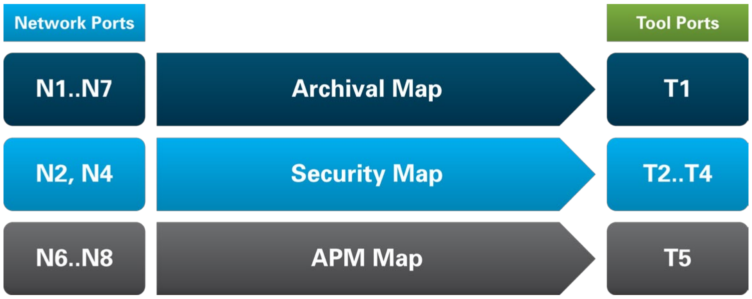
Gigamon's Unified Visibility Fabric™ architecture allows pervasive visibility across physical and virtualized networks. By centralizing and expanding the reach of tools that manage, analyze, and secure the network, IT organizations not only can manage and secure their network more efficiently, but also can provide traffic visibility as a service (VaaS) to other departments.

Role-based access controls (RBAC) allow network administrators to open the Visibility Fabric architecture as a resource to be shared across multiple organizations. Security, application performance, business services, network performance, billing, legal, and other groups all require visibility into the production network. RBAC provides the selective access to the network so that these groups can act independently and securely.

Access to the Visibility Fabric architecture is often needed on an ad hoc basis, triggered by specific events, problems, or mandates. RBAC enables users to take action without having to request access, schedule a change window, and/or obtain the assistance of a network engineer. Some IT organizations prefer to maintain complete control over the visibility of traffic flows and not allow anyone outside their group to have access. However, managing multiple daily requests for access from outside organizations can overburden the team. RBAC makes IT organizations more efficient by pre-approving access without having to worry that activities of ad hoc users will disrupt established traffic flows.

Flow Mapping Technology

Gigamon's patented Flow Mapping® technology allows users to define which traffic arriving on network ports should be sent to which tool ports. By creating flow maps and assigning map rules, users can include or exclude traffic based on IPv4/IPv6 addresses, application port numbers, VLAN IDs, MAC addresses, and more. With the latest release of H-VUE operating system 3.1 for GigaVUE HD Series products, RBAC complements Flow Mapping technology by allowing users to define maps connected to their assigned ports and prevent other users from altering their maps. Users can share access to network ports, create their own maps, and send the traffic to their tools.



Network Ports		Tool Ports
N1..N7	Archival Map	T1
N2, N4	Security Map	T2..T4
N6..N8	APM Map	T5

Figure 1: Example Flow Map

Ability to define which traffic should be sent to which tool ports egress filters are a convenient way to limit which traffic is sent to the tools while keeping the original map in place. Tool port owners can change their egress filters even if they lack access rights to change flow maps. This allows network engineers to maintain security and control of the traffic that is accessible by the tools while allowing the user to focus on the specific IP address, application, etc. that they need at any given moment. In Figure 1, multiple groups or users can attach their flow maps to the same network port resource (i.e. N2 through N7), have independent operation, and not impact other groups' or users' flow maps.

Access Levels and Locking

Individual users are assigned to user groups. User groups are given access to network and tool ports at the following levels:

- Read only
- Read/Write
- Administrative

Read-only access is for users who only need to monitor the traffic flows, but without any rights to change them. Read/write access allows users to add and edit maps associated with the ports in question. Administrative rights include read/write privileges in addition to being able to change the port settings and type.

In a typical scenario, application- and tool-based user groups would have administrative rights to their tool ports while having read/write access to network ports.

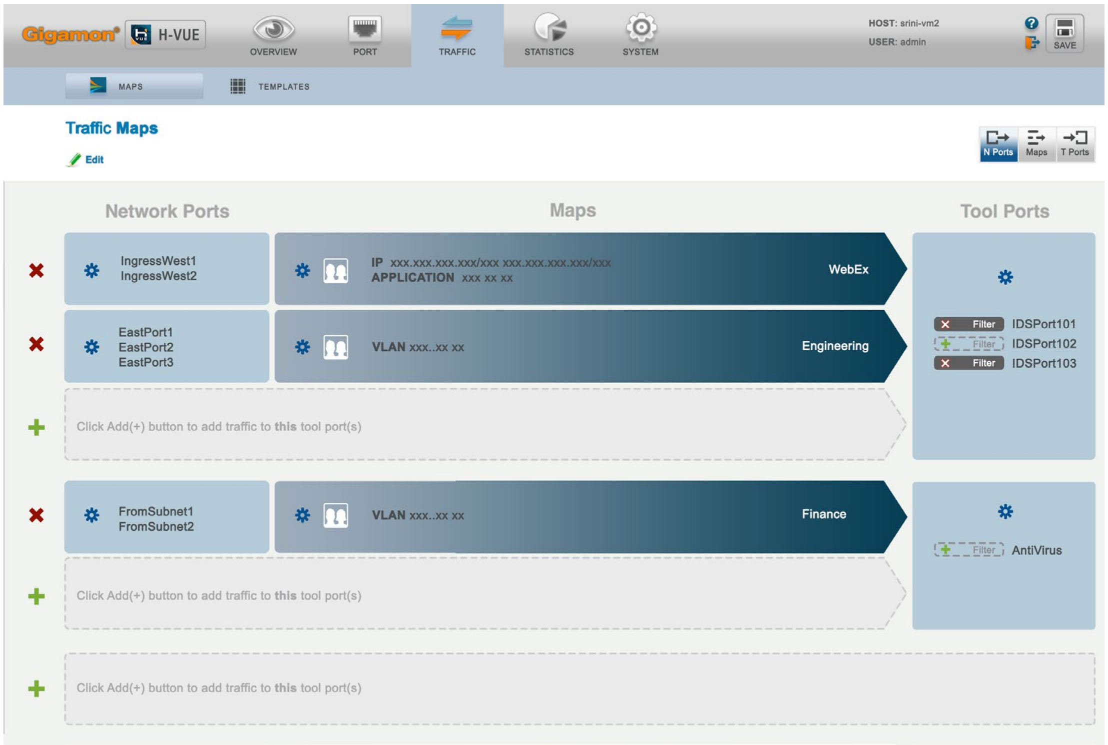


Figure 2: GUI traffic diagram

Once a map is created, users can create a lock that prevents other users from changing the map and thus preserve the traffic flowing to a particular tool port or group of ports. The lock can be shared with other users, allowing them to make changes. System administrators always have the right to remove locks and free up resources.

RBAC is also designed to work with TACACS+, Radius, and LDAP, providing local authorization once users have been authenticated.

Simplified Workflow

The architects and engineers who maintain and administer the Visibility Fabric architecture have much more experience configuring traffic flows than users who have specialized knowledge of their applications and monitoring tools. These users require an interface to the Visibility Fabric architecture that allows them to log in and define their traffic flows quickly and efficiently so that they can begin analyzing the traffic as soon as possible.

Gigamon's GigaVUE H Series graphic user interface H-VUE is specifically designed for the ad hoc, application-focused user. Users can identify at a glance the traffic that is mapped to their tools. The workflow has been streamlined to minimize the steps required to define flow map rules, add network or tool ports, or remove unnecessary maps.

About Gigamon

Gigamon provides an intelligent Visibility Fabric architecture to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

For more information about the Gigamon Visibility Fabric architecture visit: ***www.gigamon.com***