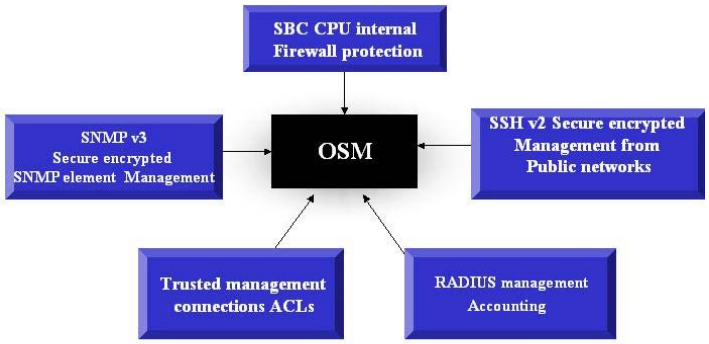
OptiSwitch Master® - Secure Management

Introduction

OptiSwitch Master® positioning in carrier and enterprise networks provides a fundamentally high security environment. The OSM incorporates an easy-to-use set of tools to simplify the network management on one hand, while preserving a superior and uncompromisingly secure environment on the other hand.

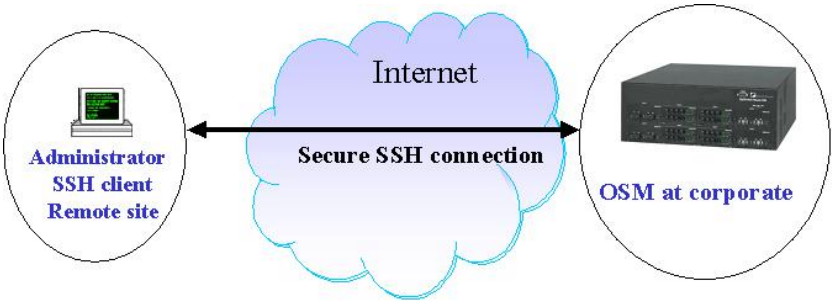
To protect the OSM from unauthorized access by remote users, the following security features are implemented:

- SSH v2 for secure remote connection
- SNMP v3/Multiple Authentication levels
- Trusted management connections & ACLs
- RADIUS –authentication and accounting
- CPU Internal Firewall



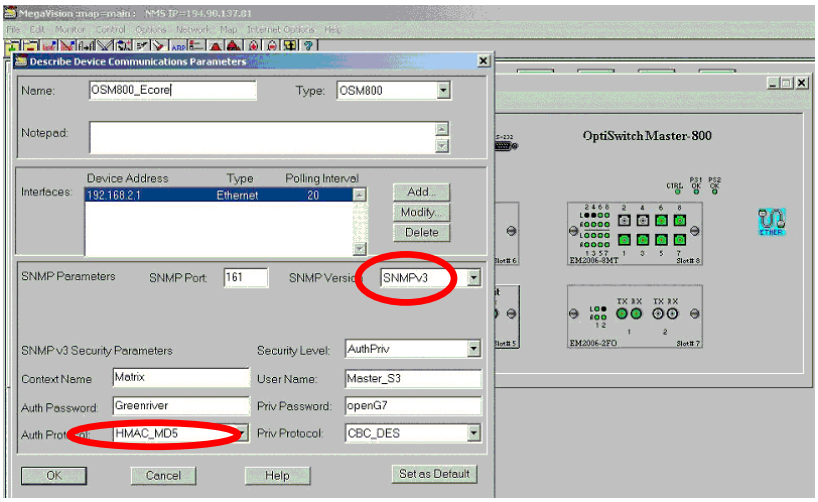
SSH Remote Management

SSH protocol replaces Telnet, enabling remote secure management communication over an unsecured channel, such as the Internet, in order to configure and troubleshoot the OSM . This valuable management protocol prevents a scenario in which a hostile user can force termination of a session, or decrypt the traffic (passwords), or hijack the connection. OSM implements SSH v.2 but can be customized for backward compatibility to SSH v.1. SSH v.2 implements an enhanced algorithm for host authentication. This algorithm prevents eavesdropping during the login process and ensures end-to-end security.



SNMP v3 Management

The SNMP protocol is considered to be non-secure because of the nature of its community strings and lack of password protection.
The traditional strings method which sent unencrypted data for authentication over the network, can be "sniffed" by hackers to exploit those links for harmful network manipulation. This may not extend to modern networking requirements and as a matter of fact the new SNMP v3 greatly improves security by implementation of encrypted community strings with DES/MD5 hashing.
It also provides user-based access control to SNMP data, as shown in MRV's MegaVision NMS window below.



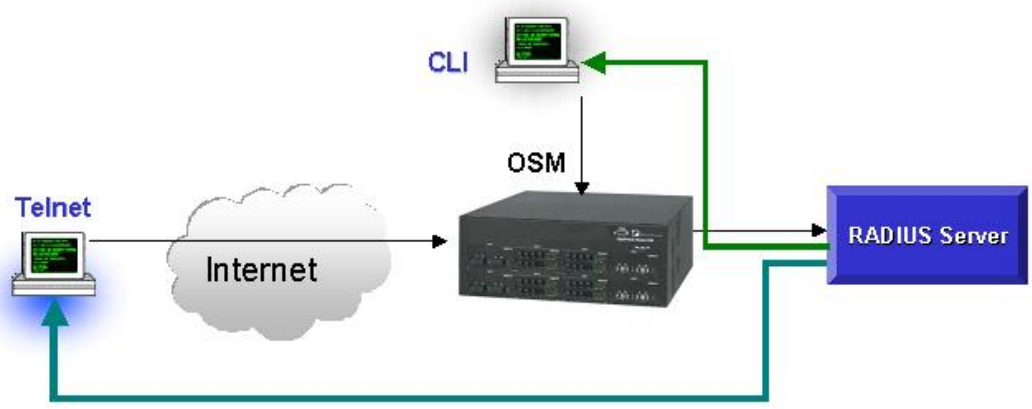
Multiple Authentication Levels

SNMP management access is restricted to authorized personnel in the following hierarchical structure of access levels:

1. Admin
2. Write-read
3. Read-only
4. Not-config - device identification only

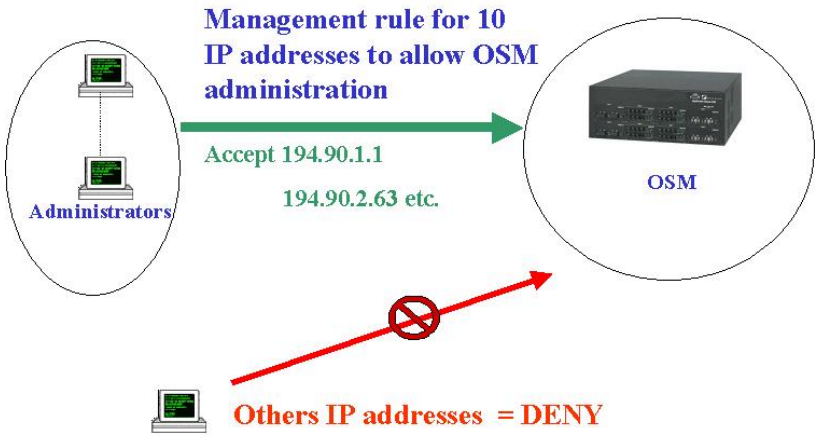
RADIUS -- Authentication and Management

RADIUS (Remote Authentication Dial In User Service) management allows a single "database" of users (administrators) for authentication (verifying user name & password). The RADIUS server collects logging information of the typed commands and authorization level changes. This information is gathered in a special log file that enables a supervisor to analyze all activities of all administrators and to track abnormal events.
The log maintains a detailed record of all interactions performed by each administrator. This provides a base for performing administrative analyses and event tracking.



Trusted Management Connections ACLs

The OSM provides the option for access to the OSM management interfaces by multiple administrators. This feature is typically implemented within an organization's network boundaries.
Trusted management connections can be configured in addition to the encryption options of the abovementioned protocols. The OSM can be configured to trust up to ten IP source addresses or subnets per protocol for administration access and drop any other IP source that attempts to access the CPU.
Enforcement of strict element management by SNMP, exists in a rule that can specify source addresses per community, which creates an additional protective shield against spoofing attacks.



Access Control Lists

OptiSwitch Master® offers a wide range of traffic filters that can be applied to the subscriber's traffic to ensure data integrity. Based on various differentiators (such as, 802.1p/q tags, IP source/destination/subnet address, and TCP/UDP ports), an access filter can be configured to ensure that only authorized subscribers enjoy certain resources. After such rules are defined, the access management system performs the custom filtering of every IP frame or stream of frames in real-time.
In conjunction to ACL rules, a large number of users have their own isolated pipe towards the central applications, thus eliminating any broadcast malicious attacks between close or grouped users. Another scenario is that in most of the applications servers are connected by Gigabit interfaces, which exposes them to attack by a single user, thereby consuming the whole Gigabit bandwidth, i.e., Denial of Service (DoS) attack. By rate-limiting (policing) the traffic, we can ensure that the servers are protected from this attack and not flooded with spoof traffic, and remain available at all times.

Since the OSM applications include typical scenario of the Layer 2 learning mode, significant threat might be encountered if the number of entries overflows the Learn Table. In public, large-scale, Layer 2 networks, the issue of DoS caused by a few hostile users who bombard the network with random Source MAC addresses, is unacceptable since forwarding can become severely impacted. OSM enables ACL configuration where the number of MAC addresses that one user can generate is limited. Such a restrictive rule ensures that the service will not be affected by users.

SBC CPU Internal Firewall

The networking industry has defined two major concepts; Data plane and Control plane.
The Data plane impacts forwarding mechanisms in network processor, while the Control plane operates at the instruction layer. In order not to abuse the instruction layer, the design of internal firewall creates default block point ("turn-off") for all open ports to any attempts of forwarding and management access, while all packets rejected by internal firewall are logged. The administrator applies his management policy rules that open explicit necessary tasks, and has the complete control over traffic and management resources. In addition, powerful logging service mechanisms maintain a log file report on any failed attempts to log into the management, and all successful and unsuccessful logins are logged using an internal Syslog service or redirected to an outbound Syslog server.
In the abovementioned scenario, an instant trap is sent to alert to an attempt of attack and various remedial actions can be taken.

Conclusion

Today's network infrastructure demands a tight security policy, the positive impact being high network availability as reflected directly in the business flow cycle throughout the network.
OptiSwitch Master® offers highly controlled intelligent management routing, incorporated with advanced hardware and software architecture to address security needs and, at the same time, concurrent sophisticated flexibility. The security features reflected in the OSM product line, is just one example of MRV's ongoing standing commitment to meet new security challenges and to satisfy both customer needs and market demands.

For more details, please contact:

Zeev Draer
OS&OSM product manager
zdraer@mrv.com