



## *Using Network Address Translation (NAT) for Redundant ICON<sup>®</sup> Management Connections*

Rhett Smith and Robert Meine

---

### **INTRODUCTION**

Management systems that are separated by significant distances from the devices they manage are more prone to connection loss due to network issues. Adding a redundant connection can reduce downtime by providing a failover path. The ICON<sup>®</sup> Integrated Communications Optical Network, as a wide-area network (WAN) technology, can span large distances, so it benefits from redundant connections. The ICON and its management software, SEL-5051 Network Management System Software, are often on different subnets. Therefore, the redundant connections need to span subnets. The ICON enables in-band management when all nodes are on the same subnet. This allows the operator to see all nodes in the system when connected to any one node.

This application note explains how to use network address translation (NAT) to add a redundant connection to a dynamic routing network where the SEL-5051 Software and the ICON are on different subnets.

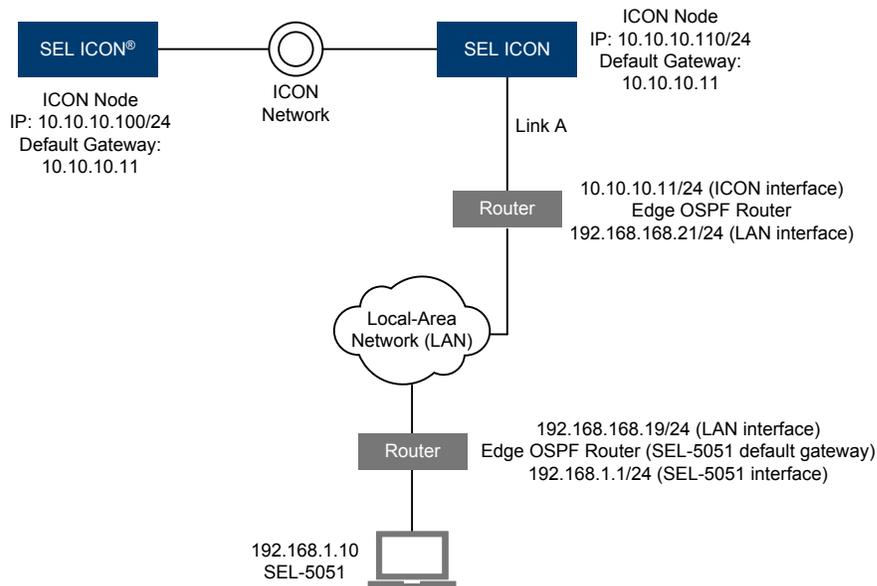
### **PROBLEM**

To detect loops, ICON devices learn media access control (MAC) addresses then alarm and discard packets if the traffic came from a learned MAC address but appears on a different port than the one stored in the MAC table. This behavior prevents some loops, but it also prevents the use of router redundancy and switch redundancy technology such as Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP). Adding a redundant route from the ICON node subnet to the SEL-5051 Software subnet must be solved using other technology.

SEL-5051 Software can automatically use multiple routes through the default gateway because it has only a single management interface to the network for any route. The ICON network can have a management connection to each node, but it can only use a single default gateway for all nodes. In a failover condition, the route through the default gateway may no longer reach the SEL-5051 Software, resulting in lost traffic and negating the benefit of the redundant route. Therefore, any solution needs to consider the single default gateway of the ICON.

## SOLUTION

The diagram in Figure 1 shows an example network, with a cloud representing a network of routers using a multipath-capable dynamic routing protocol such as Open Shortest Path First (OSPF) to connect the SEL-5051 Software with the ICON. Note that the ICON devices are on a different subnet than the SEL-5051 Software.

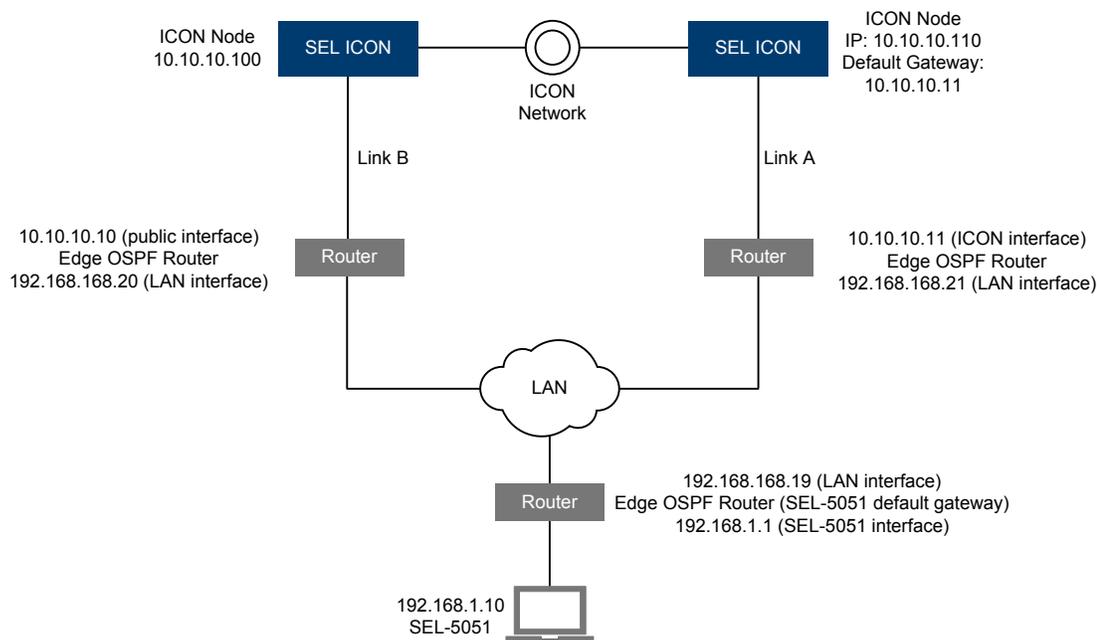


**Figure 1 Network With Single Management Interface to ICON Network**

To set up the primary connection to the ICON network, you need to configure a connection between a router and an ICON node (shown as Link A in Figure 1). The router and the ICON nodes all need IP addresses in the same subnet for in-band management. You must set the default gateway setting on all of the ICON nodes to the IP address of the router, as shown in Figure 1. On the SEL-5051, one or all of the IP addresses of the ICON nodes should be entered as network entry points.

To add the second connection, you will use outbound NAT. NAT multiplexes multiple host connections through one host by modifying the source address of traffic going out through the public interface to match the address of that interface. With NAT enabled on the router, traffic from the SEL-5051 Software appears to the ICON nodes with the router's public interface IP address, which is on the same subnet as the ICON nodes. The ICON nodes no longer have to use the default gateway and can now send traffic to the public interface of the router. The router then replaces the destination address and sends the traffic to the SEL-5051 Software through the redundant route.

To set up the redundant route, you need to add a connection between a different router and ICON node. Next, you need to configure the router to use NAT by setting up a public interface and corresponding NAT rules. Note that the public interface is the interface connected to the ICON nodes. The redundant route is labeled Link B in Figure 2.



**Figure 2 Network With Two Management Interfaces to ICON Network**

Neither the ICON nodes nor the SEL-5051 need to be configured to use the new route; the routers provide the failover automatically. For example, for a link failure in the primary route, the routers on the failed link detect a connection problem and then flood advertisements that no longer include the broken link to neighboring routers. The neighboring routers then send updated flood advertisements to their neighboring routers (and so on) until the entire routing domain has synchronized. The SEL-5051 default gateway then routes traffic to the next hop in the redundant route. Keep in mind that the failover time depends on the dynamic routing settings and the state of the routing domain.

The redundant route and the primary route should be designed to be as independent as feasible so that any issues in the primary route do not affect the redundant route. For example, both routes might fail when using the same cable for both routes if that cable fails or when powering routers from the same power source if that power source fails. The routing domain is capable of hot failover, but any dependence between routes can mean that the same issue disables both routes. Redundant routes should be tested before use.

Additional redundant routes can be added using the same two steps: add an additional connection and set up NAT on the router. NAT can even be used on the original connection to eliminate the need for a default gateway on the ICON network altogether.

The routers only provide a redundant connection to a subnet, not a host. If the interface to the subnet is up, then the router considers the subnet reachable. If possible, a cable should be placed directly between the router and the ICON node with no intervening equipment (such as a switch).

## CONCLUSION

Using the solution presented in this application note, adding an additional network connection only requires adding a connection between a router and an ICON node and configuring NAT on the router. No changes to the SEL-5051 Software or the ICON nodes are necessary. This solution can be repeated to add redundant routes for additional management connections to the ICON network.

## FACTORY ASSISTANCE

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.  
2350 NE Hopkins Court  
Pullman, WA 99163-5603 USA  
Telephone: +1.509.332.1890  
Fax: +1.509.332.7990  
www.selinc.com • info@selinc.com

