Case Study

March 28, 2006

Ethernet Soft Permanent Virtual Circuit— A RAST-Assisted Feature

Edwin Hoffman, CSA

RAPTOR NETWORKS TECHNOLOGY INC

Case Statement

This case study discusses the inherent advantages of Raptor Adaptive Switch Technology (RAST™) when implementing Layer 2 Access Control Lists (ACLs). These ACLs are prevalent in virtually all switches used today.

This simple feature allows a user to effectively “lock” a MAC address pair together on a particular physical port pairing in a switch and, in a normal switch, creates two MAC addresses that are either allowed or denied access to each other through the designated ports.

Raptor RAST Advantage

Definition:

Permanent Virtual Circuit, a virtual circuit that is permanently available. The only difference between a PVC and a switched virtual circuit (SVC) is that an SVC must be reestablished each time data is to be sent. Once the data has been sent, the SVC disappears. PVCs are more efficient for connections between hosts that communicate frequently.

PVCs play a central role in Frame Relay networks

Source: Webopedia

In a RAST network cluster of switches acting like a single switch over long distances, this simple feature becomes analogous to the Frame Relay or ATM technology Permanent Virtual Circuit (PVC), in that this circuit is permanently available, but is virtual in nature. To further increase the use of this feature using RAST's ability to create resilient connectivity between sites, the PVC can automatically reconnect between nodes after a path failure, and therefore becomes analogous to ATM's Soft Permanent Virtual Circuit (SPVC). Given that Ether Raptor can also assign priority and QoS (DiffServ) to this stream, the analogy to ATM technology is more apparent.

Of course, an Ethernet switch cannot ever perform the functions of an ATM switch. Even if it could, the expense would be prohibitive. There are some ATM switches that can transport Ethernet frames (Payload Agnostic ATM switches), but these are also very expensive.

Where can this feature be considered useful? Consider the following possibilities:

- Any network that has specifically directed video traffic (security or surveillance video) where the video stream will always be directed to a specific target, but it must also be resilient.
- Disaster Recovery networks where storage traffic must always travel between two specified points and must also be resilient.
- Cluster computing systems that need the lowest possible latency times between systems.

All of the above can be virtually “hardwired” across a RAST network in the equivalent of an SPVC link that can recover path faults and be rapidly switched to another path.

Using this topology:

- Applications do not need to use IP addresses to communicate (using only MAC addresses) because their network port is effectively connected only to another system’s network port.
- Security is increased because no other system can communicate with either of the systems unless specifically permitted.
- Latency is reduced because the systems have effectively been hardwired together.

Figure 1 shows five workstations that are connected through SPVC to an application server. External systems cannot even ping the servers or workstations because they will not accept packets from any location except the designated nodes.

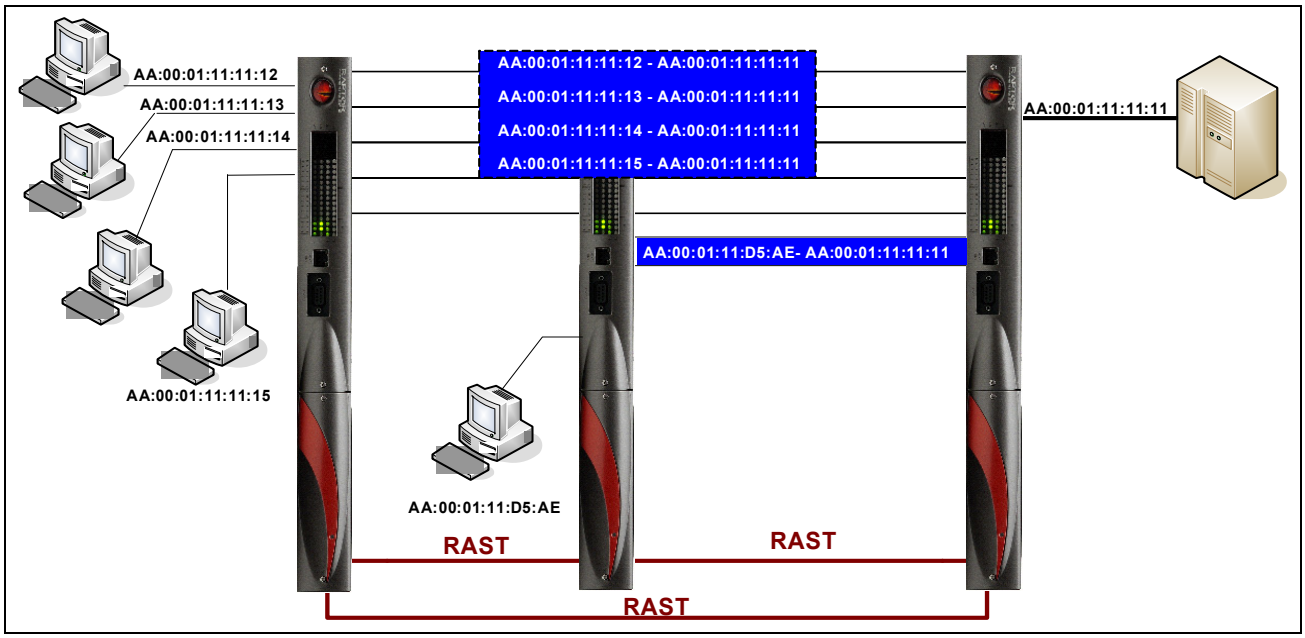

Figure 1. Ethernet Switched Virtual Circuit

The workstations cannot “see” anything else on the network unless given permission. These connections are resilient because any loss of link between the switches will simply switch the data around the other way. The application is resilient because workstations can be connected on any member of the RAST switch cluster, therefore a switch failure cannot kill access to the application, but still no other unauthorized node can even see the application server.

This security provides even greater security than a VLAN network because accidental insertion in a VLAN-capable port breaks any VLAN security that exists. If any port is used (even a port defined as being able to support this feature), the node MAC address will prevent access to the application.

Consider the following scenario...

A company with three buildings installs a RAST network to connect those buildings together. They require a very secure low-latency resilient connection between nodes in all three buildings to reach an application, which is operating in one of the buildings.

A number of nodes in any of the buildings can be easily “SPVC'd” to the application system by using Layer 2 ACLs over the RAST backbone. Path resiliency is carried out by RAST automatically switching traffic from failed links to working links, all the time retaining the secure nature of these SPVC links.

Further application resiliency can be obtained by letting the application operate in a parallel fashion (such as an Oracle parallel server), and granting MAC access rights to both system from all secure workstations.

QoS can be applied to these streams because the very same Layer 2 ACLs allow the streams to be assessed for DiffServ processing by other parts of the Raptor switches, and for that QoS to be applied back as CoS priorities.

Case Summary

Is the Ether-Raptor switch operating like an ATM switch? Yes and no. It is not an ATM switch, yet it can emulate some of the more useful capabilities of an ATM switch without the concurrent cost of the switch. Enterprising IT engineers can make the concept work to the best advantage of the company employing it.

Corporate Headquarters: 1241 E. Dyer Road, Suite 150 Santa Ana, CA 92705

Phone: 1-866-RAPTORZ (727-8679) /Fax: 949-623-9400 / Web: www.raptor-networks.com / E-mail: info@raptor-networks.com

CS1400 03/28/06