

VeroTek

“Technology Working for People”

5/8/2007

Multicast Video over VPN Project

Overview

VeroTek was tasked by a customer to review Multicast over VPN capability, and get that capability configured. The technology issue driving the project was the requirement to multicast video and sensor data streams from the sensor sites down to the respective display and analysis locations, without the bandwidth issues that would be presented by multiple unicast data streams. While Multicast in general, is a well understood technology, Multicast over an inherently point-to-point VPN link presents technical challenges.

Test Environment

The test mock-up was established in the VeroTek Test Lab to facilitate controlled troubleshooting, and access to both web and manufacturer resources. The drawing indicates the logical diagram of the test bed, and the picture shows the equipment layout. The “right” side of the drawing and bench represent the “A” environment with a Cohu B&W camera feeding into a Pelco controller, a Cisco switch and a SonicWall 4060. A laptop is also present on this segment to allow the use of the National Laboratory for Applied Network Research (NLANR) “*iperf*” network measurement tool.

The microwave link is simulated with a crossover (red) cable between the SonicWall WAN ports. The “left” side of the bench represents the “B” environment, with the SonicWall 4060, Cisco switch and two laptops. One of the laptops is running the Camera Control software, and the other is running a browser looking at the Pelco viewer. In addition, this laptop has SolarWinds running network performance monitoring software, and the “*iperf*” module in “receive” mode.



VeroTek

“Technology Working for People”

Procedure

The first step was to reset the SonicWalls to factory default settings, and then connect the two SonicWalls in a pure “router” mode with support for Multicast traffic. In this configuration, the Cohu/Pelco was able to transmit multicast video frames to the Pelco viewer on the other side without a problem.

The next step was to again reset to factory defaults, and then establish a VPN tunnel between the two sides, as currently used in the real system. The purpose of the VPN tunnel is to provide encryption of the data stream prior to its transmission over the microwave link. The VPN link was established and confirmed, with multiple ping and telnet sessions back and forth between the two sides of the network.

At this point, the Multicast traffic was no longer able to cross the link. The Pelco viewer on the left could see video if it connected through “Server Push” mode, which uses http connections over the VPN link. B. Song was observing this same symptom in his initial field tests. At this point, the team followed the SonicWall Tech Note (attached) for establishing Multicast over VPN, but several problems were encountered. The team opened a trouble ticket with SonicWall and spent the next day and a half trying various alternatives. The following is the summary of lessons learned re: the SonicWall.

1. The note is not explicit about what interfaces need Multicast enabled. The initial try was to enable on both LAN and WAN, and that turned out to be a mistake. When enabled on the WAN interface, the SonicWalls go into error mode (quick flashing alarm light) and show “spoofed traffic” in the error logs. For our application, we found Multicast should only be enabled on the LAN interface.
2. The SonicWall has “Require IGMP Membership ...” checked by default, and the Tech Note implies it should be left that way. More on this issue later, but unless one is 100% certain their apps support IGMP “join”, this box should **NOT** be checked.
3. The Tech note also implies that a multicast address object is only required if one has checked the “Enable reception for the following addresses” function. In our tests, we found that the multicast object had to be created in either case. So, create a multicast address object for the desired address (i.e. 239.96.0.1) on both SonicWalls You’ll need it later.
4. In summary, for Multicast over VPN. On both sides, enable multicast on the LAN interfaces [Interfaces – LAN – Edit – Advanced]. On the “sending” SonicWall, create a VPN policy from “LAN Subnets” to an object that has both the far side network address and the desired multicast address object. The destination gateway is the WAN address of the far side SonicWall. On the “receiving” SonicWall, create a VPN policy from an

VeroTek

“Technology Working for People”

object that has both “LAN subnets” and the multicast object. The destination gateway is the WAN address of the far side SonicWall.

5. At this point, the VPN tunnel should establish (Green Balls on the status screen) and multicast traffic should be passing through the link and viewable on any of the devices that are expecting traffic at that multicast address.
6. The Tech Note implies the IGMP “State Table” will reflect the multicast group to which the SW is providing support. This cost us a lot of time and frustration, because it turns out this is driven completely by the client applications on the segment. If no clients issue “join” requests, the table will never have an entry, but the SonicWall is still passing the multicast traffic.

At this point, the test environment was demonstrating multicast traffic over the VPN, and near full motion video was observable on the two laptops on the “B” or left side of the link, with no observable pixelation or frame drops. The Fluke OptiView confirmed that multicast *udp* traffic was flowing from 10.21.0.10 (Pelco controller) to the 239.96.0.1 multicast address. The SolarWinds gauges indicated the video data stream to be about 100 Kbps.

Encryption Impact

A question had also arisen re: possible negative impact of AES 256 encryption on throughput of the SonicWalls. Once we had the Multicast over VPN tunnel established and stable, we tested the links with 3DES and all combos of AES up to AES 256 and could see no appreciable differences in throughput.

Open Issues

This project highlighted for VeroTek the fact there are a couple of open issues that may be of concern to the design team, as multicast begins to be used for support of video and sensor data in larger segmented networks.

1. The first issue relates to the multicast data after it is “dumped” onto the far side LAN segment. Under the RFC’s and IEEE specifications, the destination MAC address of the Ethernet frame as it leaves the SonicWall (or any router) is the combination of the IANA reserved 01:00:5E:00:00:00- 01:00:5E:ff:ff:ff MAC range and the least significant bits of the IP address. For example, in our test, the frames were headed to 01:00:5E:60:00:01. When this hits a switch, there is no such entry in the MAC table, so the switch floods the traffic to all ports, and continues to do that forever. In a small network, this is perhaps not a problem, but the solution does not scale well and may prove problematic as we

VeroTek

“Technology Working for People”

support greater and greater amounts of multicast traffic.

The solution within the switch is one of three choices: One is to let it continue to flood or broadcast. The second solution is to statically configure the desired switch ports to receive the traffic. In the test lab, we could use the (i.e. [ip igmp snooping vlan 1 static 0010.5E60.0001 fast0/3]) command and the switch then forwarded the multicast traffic to the desired ports. This solution works well; it just requires a large degree of manual switch administration. The third and most scalable solution is to use either the Cisco Group Management Protocol (CGMP) or the vendor neutral IGMP Snooping protocol. Based on a mixed vendor environment, the IGMP Snooping appears to be the best solution. In IGMP snooping, the switch leaves it's strict Layer 2 device mode and examines IGMP packets that are flowing through it. When it sees IGMP “Membership Reports”, it makes any entry in its MAC table to send Multicast traffic to only those devices. In the lab test, we were able to confirm operation of both of the modes. When we configured static port assignments, the broadcast flooding stopped and the video went just to the desired laptop ports. Then we tested the link using the iperf software, which issues a real multicast “Membership report” or “join” request. In the test, the switch recognized the request and made an automatic entry in the MAC table, and perhaps more interestingly, the SonicWall saw the “join” and for the first time made an entry in it's IGMP state table. At that point, we were able to set the SonicWall fro “Require IGMP Membership” and the entire system worked as it should.

2. The second issue is the use or invocation of RFC 2236 Internet Group Management Protocol (IGMP) in application software developed, specified or supported by the customer. The IGMP protocol requires an end application to issue an IGMP “Member Report” or “join” request to the local segment router in order to join a multicast group. It is this “join” process initiated by the end application that drives the entire switch “snooping” capability and the router “traffic prune” capability necessary for scalable implementation of multicast. From our limited test, we could not observe the “Camera Control” or Pelco Viewer issue any such requests, which drives the short-term solution to manual configuration of the switches and routers. It would make sense on a go-forward basis to incorporate such support in vended software.
3. The third open issue is the selection or standardization of multicast addresses to be used within customer networks. In researching the multicast RFC's, several interesting caveats became known.
 - The entire range of multicast addresses is 224.0.0.0 – 239.255.255.255
 - The range 224.0.0.1 – 224.0.0.255 are confined to a local segment because they are defined with a Time-to-Live (TTL) of 1, so they can not be routed out of the segment. We should stay away from this range for routed solutions.

VeroTek

“Technology Working for People”

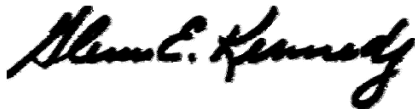
- 224.0.1.0 – 238.255.255.255 are called Globally Scoped and intended for multicast that will be on the Internet. We may want to avoid those unless we are developing a solution that needs Internet routing.
- In addition, 224.0.1.X has a number of reserved addresses, so perhaps we stay away from those all together.
- The range 239.0.0.0 – 239.255.255.255 are called Limited Scope Addresses or Administratively Scoped Addresses and defined by RFC 2365 to be constrained to a local group or organization. At first glance, these seemed like the correct match for our requirements in customer networks. I arbitrarily chose the 239.96.X.Y, but could comply with any address the customer directs.

Recommendations

In the VeroTek view, much has been learned and demonstrated by this test evolution, and we believe it provides an excellent resource for our greater team. I have attached the system diagram of the test, the SonicWall Tech Note and three whitepapers from Cisco on multicast support. On a go-forward plan, I recommend we:

- Install the SonicWall Multicast configuration with static Cisco switch support and demonstrate the correct video performance for the application.
- Give the customer time to see if they want to modify any of the recommendations and/or steer the solution to a different multicast address range.
- Based on that final addressing direction, install the same configuration in the remaining customer segments.
- In the future, modify the workstation/client software to support IGMP “Membership Report” or “join” functionality, and require the same from future purchased applications.

Thank You,



Glenn Kennedy, RCDD, CISSP
President, VeroTek