DEFENSE SOLUTIONS

Application Note: Benefits and Implementation of Network Multicast in Embedded Computing Architectures

cwcdefense.com

CURTISS WRIGHT Controls
Defense Solutions

Application Note cwcdefense.com

CURTISS WRIGHT Controls
Defense Solutions

Benefits and Implementation of Network Multicast in Embedded Computing Architectures

Introduction

Ethernet and TCP/IP networking have made tremendous inroads into military and aerospace embedded architectures over the last several years. It would be very difficult to find a processing element, I/O device, or development asset in the embedded Commercial-Off-The-Shelf (COTS) industry that does not provide Gigabit Ethernet in a prominent I/O role. With Ethernet native in virtually every COTS processing architecture and the overwhelming acceptance of TCP/IP networking in the industry, we can expect Ethernet's role to only expand.

Ethernet is used for command and control, accessing mass storage devices, data recording, sensor data interfaces, audio and video transmission, networking of legacy interfaces, logistics and maintenance support, and more. With Ethernet and the TCP/IP networking protocols common in the commercial industries becoming so integrated in COTS military and aerospace architectures, it is natural that more advanced networking capabilities from the commercial world will also become available to this industry. Network multicast is one of these networking capabilities that have been proven extremely useful in these new network-centric embedded military designs.

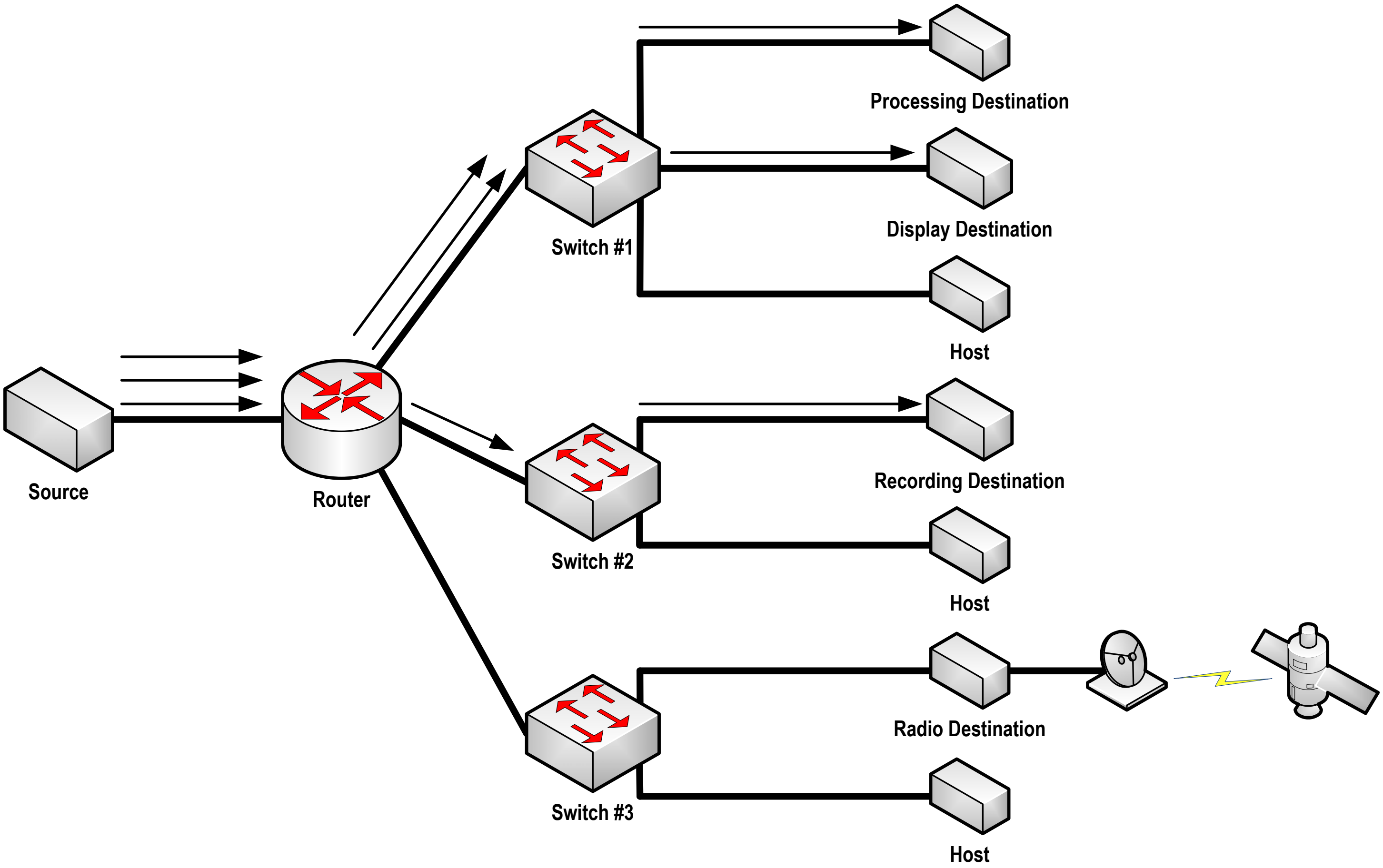
What is Multicast?

If you are familiar with using and programming Ethernet and IP networking, then you are likely familiar with unicast and broadcast traffic. Unicast Ethernet and IP traffic is normally routed and switched packet traffic where there is a specific IP source address and a specific IP address for the data. Routers inspect incoming unicast packets and forward them to switched networks or directly connected hosts that match the destination addressing in their internal routing tables. Broadcast Ethernet and IP packets provide a mechanism for a source to send a single packet to every destination host on a given local network or subnet, normally not crossing router boundaries and often being sent to hosts that do not need or care about the packet.

Unicast and broadcast cover many networking scenarios, but what if a source needs to send the same data to multiple network hosts, possibly on different local networks, without burdening destination hosts that do not need that information?

Image courtesy of DefenseImagery.mil

Figure 1: Unicast Traffic Scenario

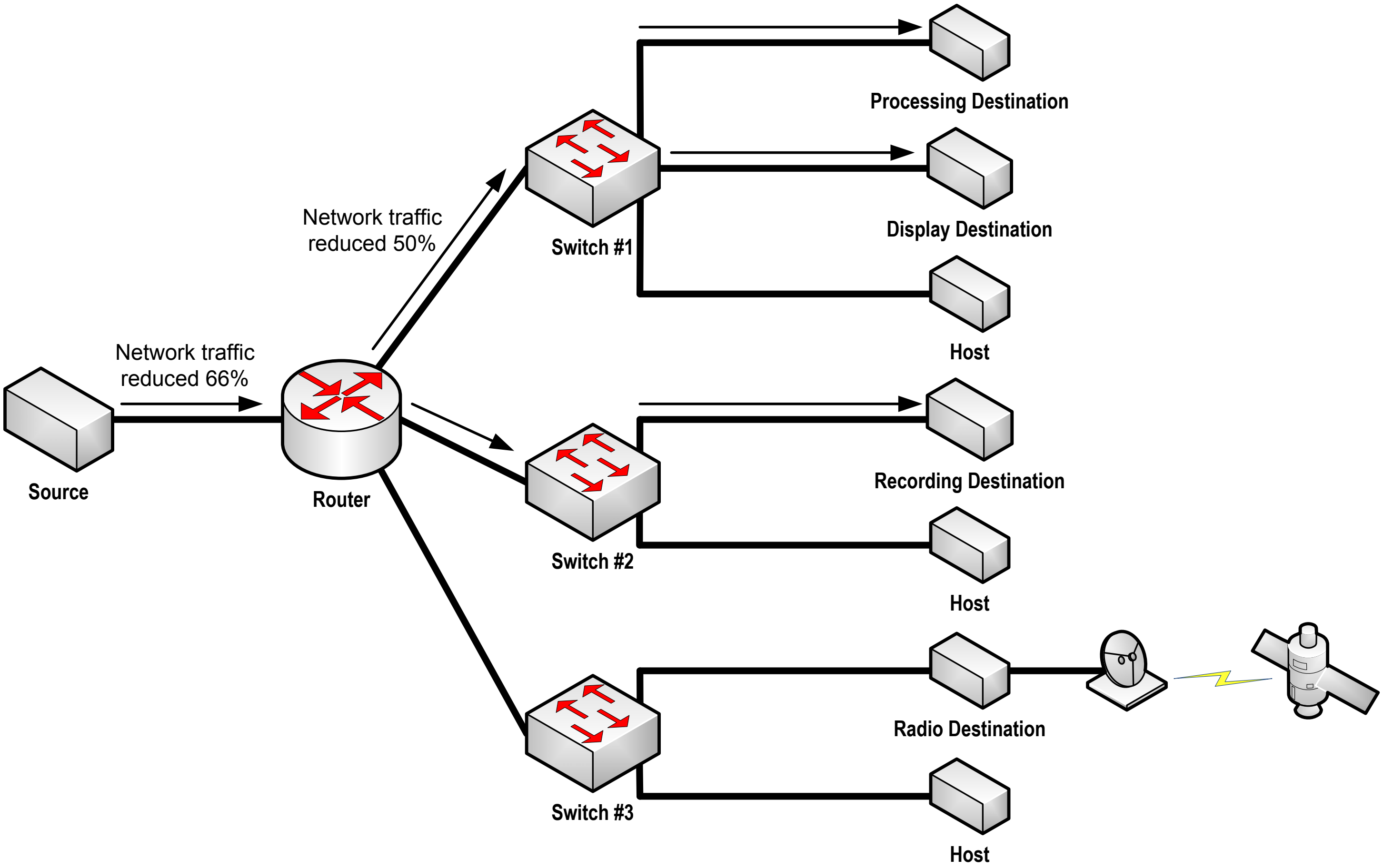


Unicast Traffic Scenario

Take the scenario depicted in network diagram of Figure 1. In this example, the source host is a sensor providing streaming uncompressed video data via IP packets to destinations of interest in the connected networks. Three destination hosts on the network (a video processor, a display device, and a data recorder) need that data in order to perform various operations. It is possible for the source to send unicast packets to each destination individually as described by the traffic arrows in Figure 1, but as is evident in the diagram, that means the link from the source to the router has three times the amount of duplicate traffic necessary and twice the traffic between the router and switch #1. It is a given that the data is uncompressed video that can consume significant link bandwidth!

In addition to bandwidth issues, latency of transmission between the various destinations may also be important, as the source will need to coordinate which destination needs to have transmission priority. If the three networks are part of the same virtual LAN it may be possible for the source to broadcast its data, but while that could minimize latency issues and reduce bandwidth requirements from the source, it would add unnecessary high bandwidth data to the other four host links on the overall network. Add to this extra bandwidth the complexity of the source needing to manage changes in the number and destinations of hosts needing its data, and it becomes clear that neither unicast or broadcast traffic are suitable for this data flow.

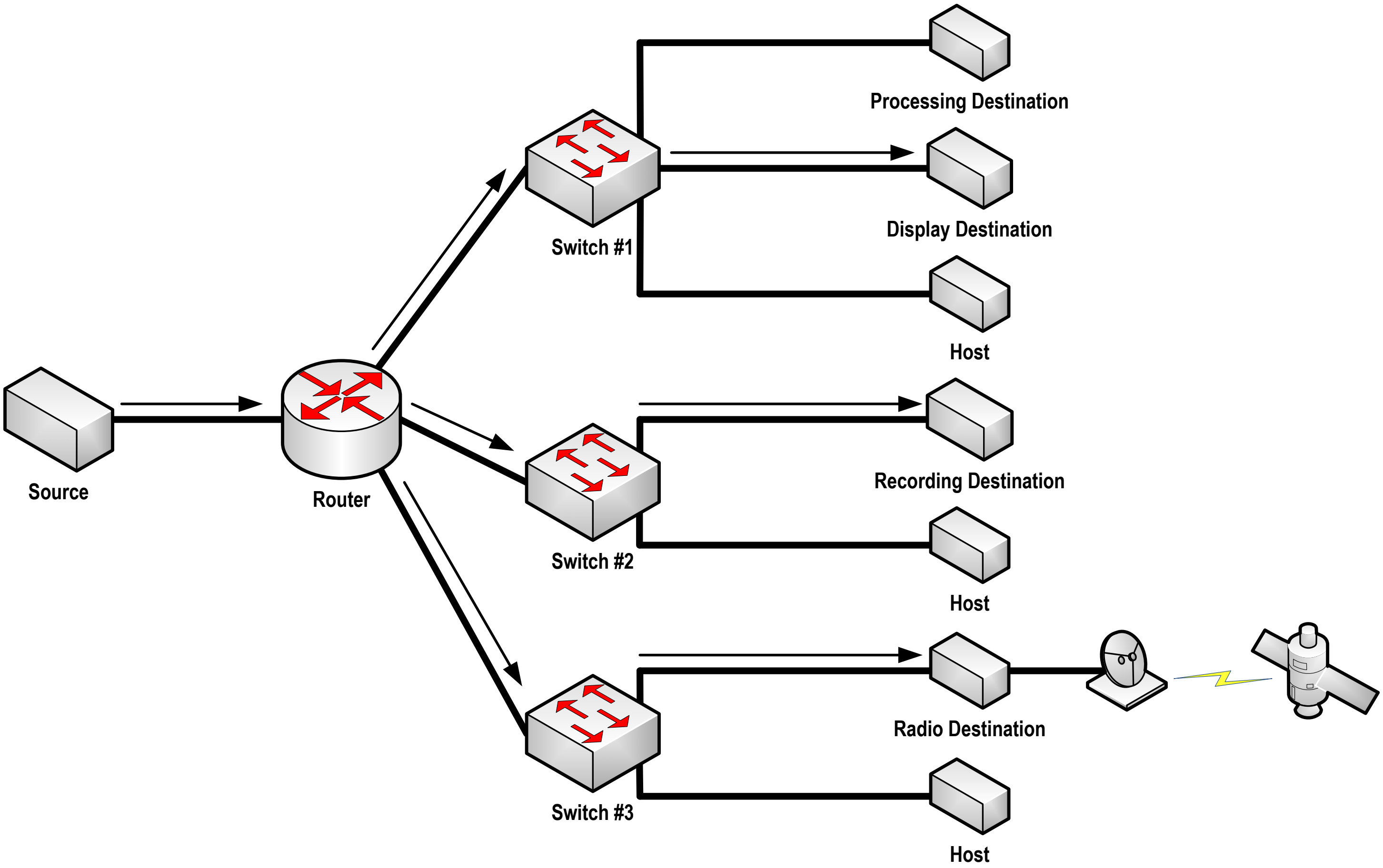
Figure 2: Multicast Traffic Scenario



Multicast Traffic Scenario

This is where multicast is useful. In a multicast enabled network, sources can send data to known multicast addresses, and destinations can subscribe to data from the same multicast addresses in the Class D IP address domain (224.0.0.0 to 239.255.255.255), and the intervening routers and switches in the network act to properly route the data efficiently and directly. Let's assume that the source sensor host is setup to transmit its sensor data to the multicast address 224.0.0.1 as shown in Figure 2. Destination hosts in the network can subscribe to that data by submitting Internet Group Messaging Protocol (IGMP) messages to their upstream switches and routers, requesting that all traffic from the source to address 224.0.0.1 be subsequently routed to that destination. IGMP message generation and scheduling is handled automatically by host operating systems that support IP multicast when the receiving socket is bound to a known multicast group Class D address, and the socket options are set for adding membership. Switches between the destinations and the router can then listen for those IGMP messages, commonly referred to as IGMP snooping, to identify which ports on their local networks to send multicast packets to that are received from the router. The result is every required destination receives the data, latency differences and latency overall is minimized, no disinterested host has their link burdened with unnecessary data, and every switch and router link only contains a single copy of the multicast data.

Figure 3: Multicast Subscribe/Unsubscribe



Multicast Subscribe/Unsubscribe

Another major advantage of multicast is the ease of run time reconfiguration of the subscribed destinations. Assume that the processing destination no longer needs the video data from the source, but the system needs the video forwarded to a radio where it can be compressed and transmitted off platform (see Figure 3). Both the processor and radio only need to issue the appropriate IGMP message to unsubscribe and subscribe respectively to the 224.0.0.1 multicast address to reconfigure the network appropriately. Upon receiving the unsubscribe from the processing destination operating system (generated explicitly by application socket option settings or automatically by the closure or unbinding of the socket from the multicast group address), the router knows it still needs to continue routing multicast data to switch #1 because the display destination is still subscribed, but switch #1 through IGMP snooping knows it now no longer switches multicast data to the processor. The router will begin routing multicast data to switch #3, which will send that data to the radio destination only without burdening any new hosts on that local network. Best of all, only the destinations that need to change are involved along with the automatic responses of the network switches and router; the other destinations still receive their data and the source is not required to be informed of any changes. This allows the programming on the source to remain simple and efficient as it is not required to maintain any information about the destinations interested in its traffic.

CURTISS WRIGHT Controls
Defense Solutions

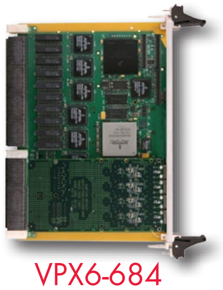
Multicast and Other Network Traffic

Multicast traffic exists on the network simultaneously with other unicast and broadcast traffic. In addition, multicast traffic can be subjected to the same Quality of Service policies and access or firewall limitations that the routers and switches exert on unicast traffic for priority and security reasons. Since multicast traffic is just a special case of standard Ethernet and IP packets, no special hardware beyond multicast-capable switch/routers is required. And while the examples described in this document only use a single router with separate switches, multicast is fully available with switch/router combinations and through and across multiple routers, as is typical with streaming data in the commercial world across the Internet.

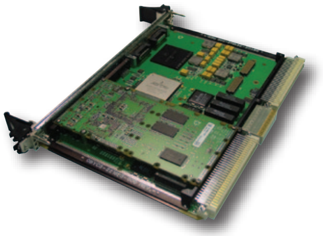
Multicast enables hosts to transmit universally needed data efficiently across the general purpose network both on platform and off platform without the need for dedicated links and without unnecessarily burdening network bandwidth. Many network-centric middleware and architecture specifications, including the new VICTORY Data Bus and Platform Services specification, require IP multicast as a central requirement for operation. As more systems, sensors, and display devices become connected via network, multicast will offer yet another means for the effective use of that network.

Curtiss-Wright's Multicast-capable Products

Most of Curtiss-Wright's switch and switch/router products are multicast-capable or multicast-allowable, meaning they can support the routing and connectivity of multicast traffic to Ethernet hosts and sources. In the 6U size, the SVME-682 and VPX6-684 provide 20 or more 10/100/1000Base-T Ethernet ports plus 10 Gigabit XAUI ports in a full featured switch/router configuration, including multicast routing and management and IGMP snooping, all fully configurable and enabled by Curtiss-Wrights standard switch/router management software suite.



VPX6-684

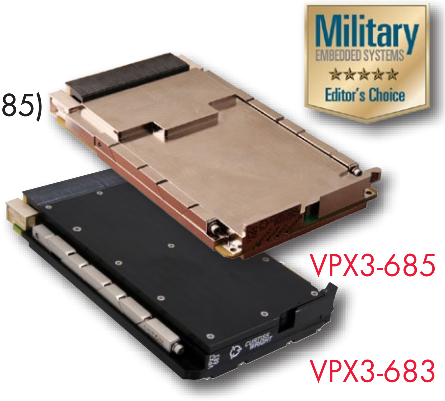


SVME-682

- 6U VME (SVME-682) or VPX (VPX6-684) form factor
- 20 ports of 10/100/1000BaseT Ethernet (24 ports for VPX6-684)
- 10G XAUI ports for network aggregation or high speed host communications
- Full featured switch/router management software suite including
  - VLANs, port forwarding, port mirroring
  - Routing, Quality of Service, Multicast (IGMP snooping and forwarding)
  - Link aggregation, DHCP, NAT, and more

In the 3U form factor, the VPX3-683 and VPX3-685 offer the exact same switch/router feature sets as their 6U counterparts, all in a smaller form factor and with either 1000Base-X and 10G XAUI or a mix of 1000Base-X, 10G XAUI, and 10/100/1000Base-T Ethernet.

- 3U VPX form factor
- 1000Base-X SerDes Ethernet (24 ports for VPX3-683, up to 8 ports for VPX3-685)
- 12 ports 10/100/1000Base-T for VPX3-685
- 10G XAUI ports for network aggregation or high speed host communications
- Full featured switch/router management software suite including
  - VLANs, port forwarding, port mirroring
  - Routing, Quality of Service, Multicast (IGMP snooping and forwarding)
  - Link aggregation, DHCP, NAT, and more
- Additional certified security and firewall features for VPX3-685



VPX3-685

VPX3-683

For smaller, remotely connected networks, the stand alone Layer 2 Ethernet switch function in the DBH-670 Digital Beachhead Vehicle Management Computer can provide IP multicast extensions from any multicast-enabled router including the Curtiss-Wright products mentioned previously.

- Small, rugged footprint at 10.5"x7.5"x3" at <5 lbs
- 16 ports 10/100/1000Base-T Ethernet
  - Standard Layer 2 switching with non-blocking operation, auto-negotiation and auto-MDIX
- Layer 2 switch management software suite including:
  - VLANs, port forwarding, port mirroring
  - Quality of Service, IGMP snooping for multicast
  - Link aggregation, jumbo frames, and more
- VICTORY architecture compliance for Data Bus and Platform Services

DBH-670

DIGITAL BEACHHEAD™

In addition, the XMC-651 Layer-2 Ethernet mezzanine switch provides an even smaller footprint addition to larger systems to extend an Ethernet networking including features suitable for exploiting the benefits of IP multicast.

- VITA 42.0 XMC specification
- 8 ports 10/100/1000Base-T Ethernet
  - Standard Layer 2 switching with non-blocking operation, auto-negotiation and auto-MDIX
- 4 ports 1000Base-X Ethernet
- Layer 2 switch management software suite including:
  - VLANS, port forwarding , port mirroring
  - Quality of Service, link aggregation, jumbo frames
  - Port flooding multicast or static multicast group support

XMC-651

For more details on our Ethernet switches and routers as well as the rest of Curtiss-Wright Controls Defense Solutions product lines please visit us at www.cwcdefense.com or contact your local sales representative.

Contact Information

To find your appropriate sales representative:

Website: www.cwcdefense.com/sales

Email: defensesales@curtisswright.com

Technical Support

For technical support:

Website: www.cwcdefense.com/support

Email: support@curtisswright.com

The information in this document is subject to change without notice and should not be construed as a commitment by Curtiss-Wright Controls Defense Solutions. While reasonable precautions have been taken, Curtiss-Wright assumes no responsibility for any errors that may appear in this document. All products shown or mentioned are trademarks or registered trademarks of their respective owners.

*Other names and brands may be claimed as the property of others.

CURTISS WRIGHT Controls
Defense Solutions

defensesales@curtisswright.com

cwcdefense.com