Laura Chappell

It's Alarming

Broadcast and Multicast Storms

In addition to helping you troubleshoot network problems, network analyzers can help you detect detrimental conditions on your company's network. For example, since broadcast and multicast storms can impact network performance, you can configure your network analyzer to send you an alarm if a broadcast or multicast storm occurs.

UNDERSTANDING BROADCAST AND MULTICAST PACKETS

A broadcast packet is sent to all of the devices on the network (0xFF-FF-FF-FF-FF-FF). A multicast packet, on the other hand, is sent to a group of devices on the network, such as spanning tree bridges. (For more information about multicast packets, see "The Making of Multicast Packets" on p. 38.) Unlike unicast packets (which are sent to a single device), multicast and broadcast packets can be identified by an odd value in the first byte of the destination Media Access Control (MAC) address field (0x01..., 0x03..., and so on). (See Figure 1 on p. 38.)

Obviously, excessive broadcast packets are detrimental to network performance because all of the devices must process each broadcast packet. Although multicast packets overload only a group of devices (such as all of the source route bridges), an excessive number of multicast packets can also be detrimental to network performance. The additional processing overhead may cause a device to deny services or drop incoming packets from other devices.

SETTING THRESHOLDS FOR ALARMS

A broadcast or a multicast storm triggers a network analyzer alarm when the broadcast frames per second threshold has been exceeded. This threshold is usually configurable, and the default setting for most network analyzers is typically 100 broadcast frames per second.

Instead of focusing on a specific broadcast rate, however, you should analyze broadcast packets as a percentage of the overall data crossing the wire. For example, if a 100 Mbps network currently supports a load of 24 Mbps, you should analyze the traffic to determine how much of the 24 Mbps is consumed by broadcast packets. If broadcast packets are 10 percent of the overall network traffic, you should find ways to control the broadcast traffic. Ideally, you want to restrict broadcast traffic to provide enough bandwidth to all of the devices that need to transmit packets on the network. I recommend that you try to keep broadcast traffic below 10 percent of the overall network traffic.

Illustration: Debbie Reynolds

IDENTIFYING THE CAUSE OF STORMS

The first step in controlling broadcast and multicast traffic is to identify which devices are involved in a broadcast or multicast storm. The following protocols can send broadcast or multicast packets:

- Address Resolution Protocol (ARP)
- Open Shortest Path First (OSPF)
- IP Routing Information Protocol Version 1 (RIP1)
- Service Advertising Protocol (SAP)
- IPX Routing Information Protocol (RIP)
- NetWare Link Services Protocol (NLSP)
- AppleTalk Address Resolution Protocol (AARP)

After identifying the source of the broadcast or multicast storm, you must examine the packets to find out which protocol or application triggered the broadcast or multicast storm. For example, if a single device is responsible for a broadcast storm, you can examine the device's broadcast traffic to determine exactly what the device was doing. For example, you can find out what the device was looking for or what the device was announcing.

Broadcast or multicast storms are often caused by a fault that occurs during the device discovery process. For example, if an IPX-based printing environment has been misconfigured, a print driver client may continually send SAP packets to locate a specific print server. Unanswered broadcast or multicast requests usually indicate that a device is missing or has been misconfigured.

Examine the broadcast traffic on your company's network. Do you see numerous unanswered, repeat queries? Do you see protocols (such as IP RIP1, SAP, and IPX RIP) that just "blab" all day even when no other devices may be listening?

Or, is the majority of the broadcast and multicast traffic on your company's network purposeful? That is, does the broadcast and multicast traffic have a request-reply communication pattern? For example, are broadcast lookups answered?

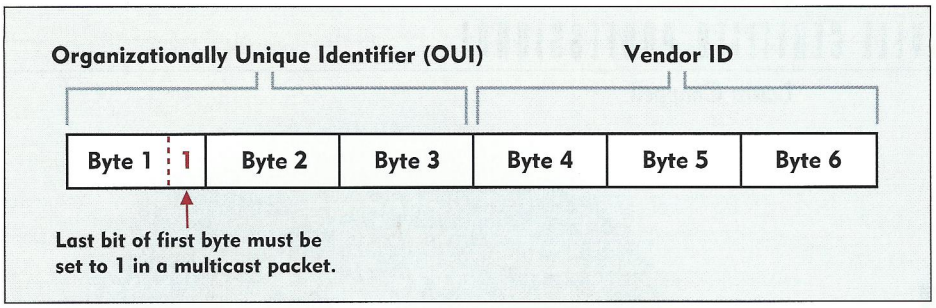

Figure 1. *The first byte in a broadcast or multicast packet's MAC address field always has an odd value.*

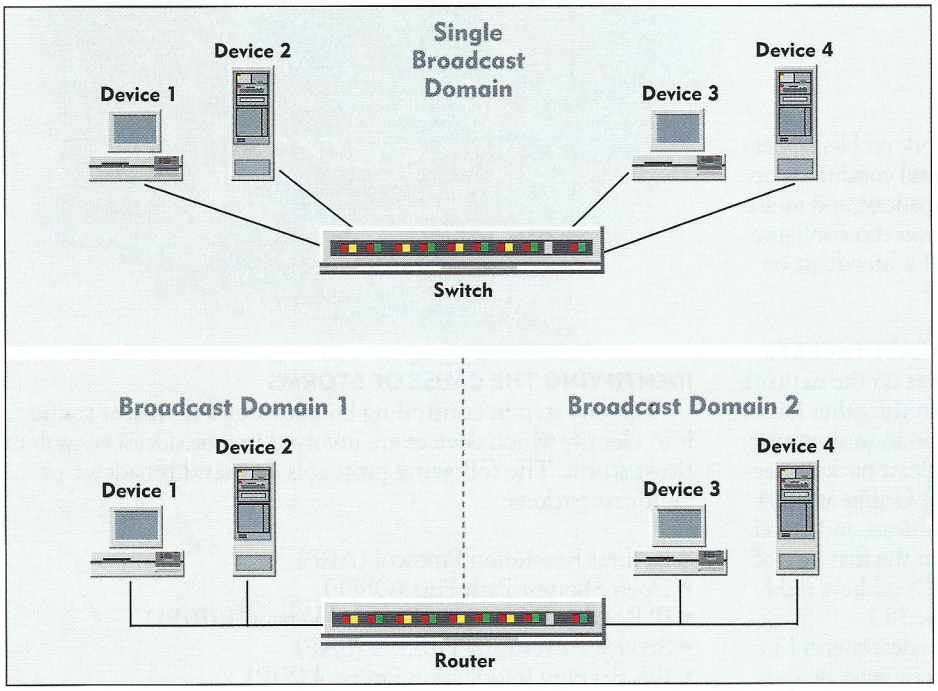

Figure 2. *The scope of the broadcast domain differs depending on the network environment.*

The Making of Multicast Packets

To better control traffic on your company's network, you should understand how devices use multicast packets. On an IP network, for example, an Open Shortest Path First (OSPF) router sends a "hello" packet to other OSPF routers on the network. The OSPF router must send this "hello" packet to an assigned multicast address, which is 224.0.0.5. (To view a list of other assigned multicast addresses, visit www.iana.org.) The OSPF router then builds a multicast destination Media Access Control (MAC) address out of this number, using the process outlined in Figure 3. ●

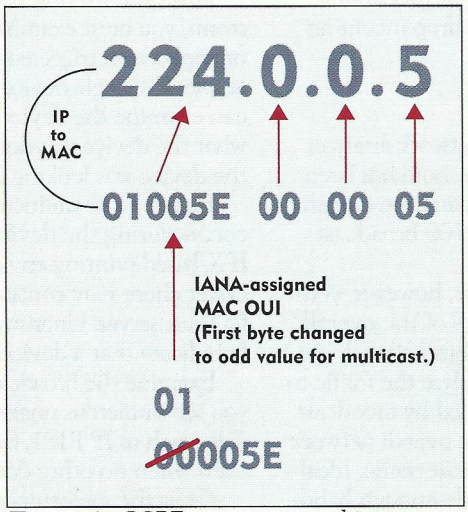

Figure 3. *OSPF routers use multicast packets to locate each other on IP networks.*

Do broadcast packets contain meaningful information? For example, if a network has numerous routers, do broadcast packets contain routing update information?

Is the broadcast rate acceptable? Does your company's network need RIP updates every 30 seconds, or can you increase the interval to one minute?

BROADCAST/MULTICAST DOMAINS

If your company's network is experiencing excessive broadcast or multicast traffic, you should also check the scope of the broadcast or multicast domain. (A *broadcast* or *multicast domain* is the range of devices that are affected by a broadcast or a multicast packet.) Understanding broadcast and multicast domains can help you determine how harmful a broadcast storm can be from any point on the network.

The scope of a broadcast and multicast domain depends, to some degree, on the network design. For example, Figure 2 shows two networks, a switched network and a routed network. On a switched network, Device 1 sends a broadcast or multicast packet that is propagated to all ports of the switch. (A typical layer-2 switch does not filter either broadcast or multicast traffic.)

On a routed network, however, a router does not forward broadcast traffic. If Device 1 sends a broadcast packet, only Device 2 and the router see the broadcast packet. If appropriate, the router processes the broadcast packet and sends a reply. Because the broadcast packet is not forwarded, it does not affect Devices 3 or 4.

Multicast traffic is a bit different in the routed environment since most routers allow you to configure the router to forward or to filter multicast packets. Although some technologies (such as Internet Group Management Protocol [IGMP]) help restrict multicast traffic to required segments of the network, many companies filter all multicast traffic at routers.

CONCLUSION

Fortunately, you can use any decent network analyzer to identify, capture, and categorize broadcast and multicast traffic. Tracking this traffic over time will help you detect if the network is being overrun by these "chatty" packets.

The senior protocol analyst at the Protocol Analysis Institute, Laura Chappell also writes self-paced troubleshooting courses (www.podbooks.com). To view Chappell's analysis information, visit www.packet-level.com. ●