Internetworking With Bridges, Switches, and Routers

When connecting computers with local area network (LAN) technology, it often is necessary to build an internetwork. What is an internetwork? It is a collection of computers which are connected with specialized electronics (bridges, switches, and routers) which allow users to communicate at great distances, at speeds approaching the high bit rates that are used on LAN’s. If an internetwork is designed carefully and properly, it will be invisible to users, since its performance will be equivalent to a single LAN.

LAN Limitations

The basic reason that we need internetworking devices is that LAN’s are not allowed to be very big. The maximum size of ethernet (the most popular type of LAN) is only about 1.5 miles. Usually, our network is bigger than that! Often, our users are scattered across distances of several thousand miles. So we can’t connect users directly with common LAN technology.

The severity of our distance problem may determine the type of internetworking device that we use. If we have a 3 mile problem, we might choose to install 2 or 3 ethernets, and connect them with a bridge. On the other hand, if we have a lot of miles to cover, we will use an internetwork built from routers.

Another LAN limitation is their inability to send more than one piece of data at a time. If two stations on a LAN attempt to transmit data simultaneously, we have a collision, and one of the computers must defer to the other. Although LAN bit rates are high, imagine the performance benefit if we could allow data exchanges between different pairs of computers to occur simultaneously.

Over the years, several types of devices have been developed to help with these problems. We’ll survey these devices next.

Bridges

The oldest type of internetworking device is called a bridge. Normally, a bridge is used when we have two LAN’s, of the same type, to connect together (see the “3 mile problem” discussed above). Two types of bridges have been developed: the transparent bridge (sometime called a “spanning tree” bridge) is used for ethernets. On token ring LAN’s, a “source routing” bridge is employed. Use of the transparent bridge is much more common, and only this type will be explained in this article.

As the name implies, transparent bridges are invisible to computers on the LAN. If you slipped into the telecomm closet in the middle of the night, broke a single ethernet into two pieces, then bridged them together, no one would know! No reconfiguration of your computers would be required. Bridges have very little configurable software in them. Most of the logic and intelligence that they do possess is implemented in their hardware. Because they are hardware-based, bridges are simple to configure, and are strong performers.

The main function of a bridge is to allow the LAN to be extended, that is, to be larger. However, it can also enhance throughput. A technical term for an ethernet is a “collision domain”. Sometimes an ethernet can have many hubs, repeaters, and links in it, but it will still be one
collision domain. If we place a bridge into the middle of this ethernet, we will subdivide the LAN into two collision domains. Since each of the two collision domains would now contain half as many computers, we would expect half as many collisions. This improves the overall performance of the networks.

Interestingly, bridges mostly configure themselves. They do this by constantly learning the addresses of the computers that are connected to the bridged LAN’s. During the learning process, an address table is built (called a CAM table), and the contents of this table are dynamically adjusted as computers are booted up or powered off. The addresses in this table are used by the bridge to perform forwarding and filtering, which means that the bridge is capable of making intelligent decisions about allowing frames to be passed to the other side (forwarding) or not (filtering). The performance of a bridge is measured in terms of the number of data frames (per second) that it can forward and filter. You can see how the filtering capability, in particular, would reduce loading on the LAN’s and further enhance performance.

Switches

The switch device is a derivative of the bridge and operates using many of the same concepts. The primary difference between a switch and a bridge is the number of ports – while a bridge will have only two ports, the switch may have 12, 24, 48, or even 128 ports. We can guess right away that the switch is used in a different way than a bridge.

The most effective way to use a switch is to connect only one computer to each switch port, although it is allowable to connect a LAN to each switch port. If we connect only computer to each switch port, we will have a collision-free network, since there are only two devices (the switch and the computer) on each link. This greatly enhances performance, because the switch will allow many simultaneous data transfers.

Like the bridge, the switch learns addresses on its own, and builds an internal CAM table that is used for filtering and forwarding. Switches require very little configuration, in fact I have met several clients that have misplaced the manuals for their switches, and have survived! I don’t recommend this, however.

The switch application is to interconnect computers equipped for LAN’s. If we want to build an internetwork across a wide-area network (WAN), we are likely to use a more powerful device – the router.

Routers

Compared to bridges or switches, the router is the most flexible internetworking device, is likely to be more complex to configure, and usually costs more. Routers are much different from bridges or switches, in that they are computers with CPU’s, software, RAM buffers, and specialized storage devices. They run a specialized operating system written to support routing (it’s not like Windows). Some early routers were in fact PC’s with custom software, but now most routers are stand-alone devices.

Unlike switches, routers are dependent on a forwarding protocol. The most common one is the Internetworking Protocol (IP), of TCP/IP fame. This is the forwarding protocol of the Internet. IP is installed and configured in the router, and it must also be installed and configured in all computers that need to use the router. Note that this means that the router is not transparent to the
computers, and in some way the router and the computers must interact and communicate with each other.

A key step in configuring an internetwork to use IP is the allocation and distribution of IP addresses. This is a complex task and must be carefully planned. Usually, IP addresses will be laid out in subnets, meaning that blocks of addresses are reserved for different portions of the network. Often each LAN is a separate subnet. IP addressing assignment on the routers must be consistent with the subnetting scheme that is selected.

A key feature of the router is its ability to communicate with other routers that are on the internetwork. This is done using a routing protocol, such as Open Shortest Path First (OSPF). Use of the routing protocol, routers can tell other routers about the subnets that are connected, and how subnets can be accessed. The routing protocol also is used to tell other routers about routing changes, such as a route that was previously up, but now is down. Routing protocols must be configured in the router, before they will operate properly. This is often a complex task.

This all adds up to a lot of configuration complexity. Routers are much more intricate than bridges or switches. However, because of their features, power, and flexibility, routers can adapt to a lot of internetworking configurations, and their use will lead to a tightly managed and efficient internetwork.
Final Comments

In this article, I’ve only scratched the surface of how internetworks can be designed and built. My goal in the development of this white paper is to explain the working of an internetwork at a very high level. I would certainly appreciate any comments or questions that you might have. Please contact:

smiths@vxconsult.com