Michael Salib 6.033 3/5/02

CSMA/CD networks offer a number of unique benefits. One such advantage is how CSMA/CD networks respond to increasing demand. Unlike traditional isosynchronous networks, CSMA/CD networks exhibit a soft capacity limit. This means that they can easily accommodate a growing number of hosts at the cost of increasing latency and reduced average bandwidth. If these costs prove excessive, users can divide the network into multiple segments connected with packet filtering bridges. The ease with which such networks can grow to meet changing user needs is due in large part to their soft capacity.

Despite such advantages, this decentralized control system introduces a number of problems. For example, without a central arbiter that can block communications, any hostile node can bring the entire network to a screeching halt. Hostile nodes may be malicious, may have broken software or may simply be misconfigured. When (not if) serious problems arise in the network, the lack of centralized communications facilities makes logging and fault isolation far more difficult.

The designers of CSMA/CD networks often go to great lengths to make the network resilient to failures in individual nodes. They do so by placing failsafe cutoff circuits in the transceivers and designing the low level interface software to ensure that the bandwidth fairness protocols are always followed. However, even if a hostile node cannot completely stop traffic because of these protection mechanisms, it can easily wreak havoc by forging packets. Rogue nodes can also seriously degrade network performance by legitimately adding excess broadcast traffic to the network. Indeed, the lack of strong authentication and host isolation has made traditional Ethernets vulnerable to a wide array of session hijacking and man in the middle attacks.

Many of these problems stem from the fact that all nodes are directly linked together. We can solve some of these problems by introducing a layer of indirection to the system. One solution would be to use centralized hubs connected to individual stations in a star configuration. This allows us to keep distributed control inherent in CSMA/CD at a logical level while reaping the benefits of centralized physical links. This change makes the network far more resilient to damaged or broken nodes since hubs can isolate overly "chatty" nodes from the rest of the network. Sufficiently advanced hubs (like modern Ethernet switches) can ensure that each node see only the traffic destined for it, thereby eliminating many security problems.

Unfortunately, this new layer of indirection brings with it several new problems. The hubs are now a single point of failure. However, given that hubs are simple, dedicated devices with no moving parts, no software, and no configurable elements, they are far more reliable than the collection of end nodes that network reliability originally depended on. Hubs can also be physically secured in ways that a large collection of end systems generally cannot.