6.17 Proxy ARP

Intranets sometimes use a technique known as proxy ARP to implement a form of security. We will first examine proxy ARP, and then see how it can be used.

Early in the history of the Internet a technique was developed that allowed a single IPv4 prefix to be used across two networks. Originally called The ARP Hack, the technique became known by the more formal term proxy ARP. Proxy ARP relies on a computer that has two network connections and runs special-purpose ARP software. Figure 6.5 shows an example configuration in which proxy ARP can be used.

![Figure 6.5 Illustration of two networks using proxy ARP.](image)

In the figure, the computer labeled P runs proxy ARP software. Computer P has a database that contains the IPv4 address and the Ethernet MAC address of each other machine on network 1 and network 2. The router and all the other hosts run standard ARP; they are unaware that proxy ARP is being used. More important, all the other hosts and the router are configured as if they are on a single network.

To understand proxy ARP interaction, consider what happens when router R receives a packet from the Internet that is destined to the IPv4 prefix being used across the two networks. Before it can deliver the incoming packet, R must use ARP to find the hardware address of the computer. R broadcasts an ARP request. There are two cases to consider: the destination is on network 1 or the destination is on network 2. Consider the first case (e.g., suppose the destination is host H1). All machines on network 1 receive a copy of R’s request. Computer P looks in its database, discovers that H1 is on network 1, and ignores the request. Host H1 also receives a copy of the request and responds normally (i.e., sends an ARP reply).

Now consider the second case where R broadcasts a request for a machine on network 2 (e.g., host H4). ARP was only intended to be used on a single network, so broadcasting for a computer on another network seems like a violation of the protocol. However, R is behaving correctly because it does not know there are two networks. All computers on network 1 will receive a copy of the broadcast, including P. Computer P consults its database, discovers that H4 is on network 2, and sends an ARP reply that