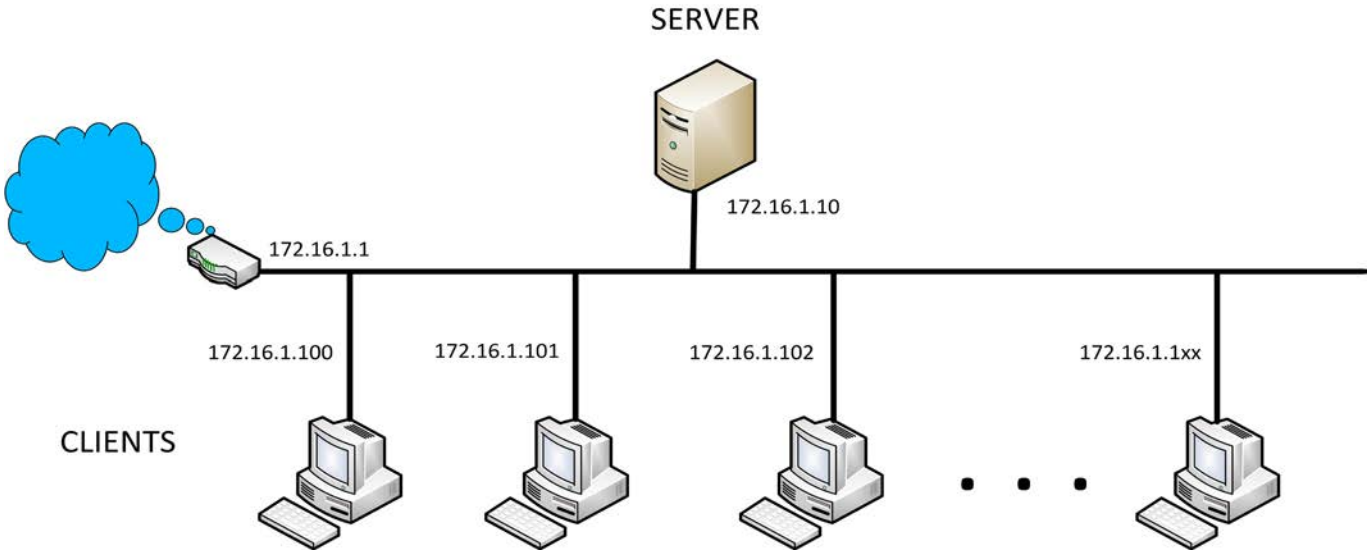
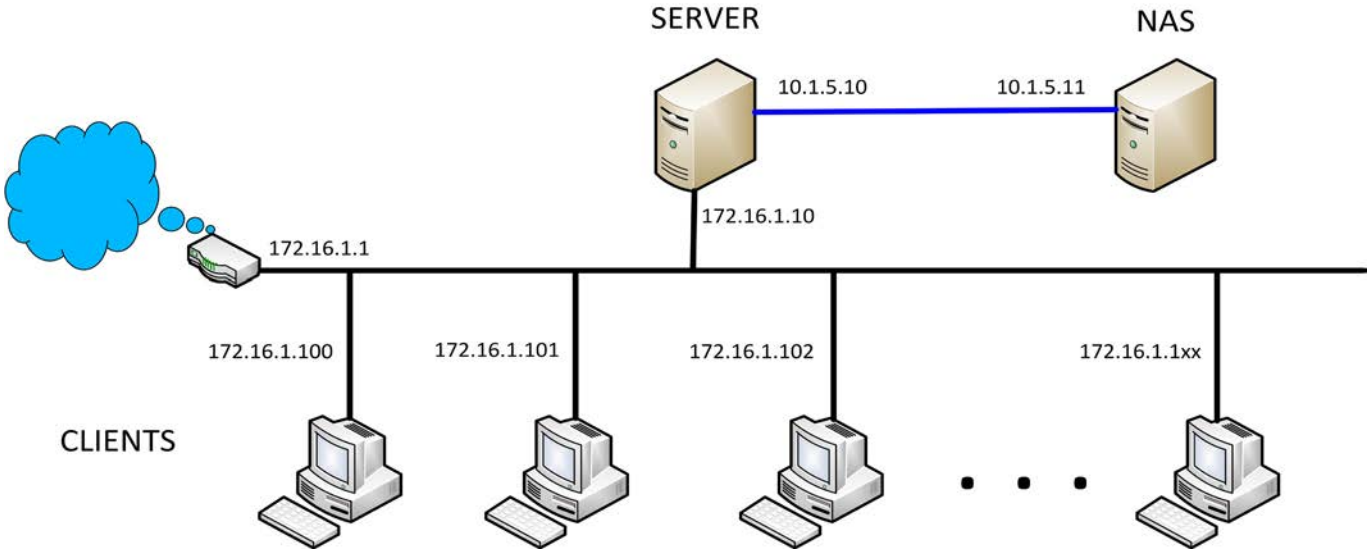
Using a NAS for Disaster Recovery

In the flat network shown below, client application files are stored on the file server. If this server is mapped as a network drive by the clients, your enterprise is only one click away from a malware attack from a malicious ransom-ware virus. If any client clicks on the wrong email, every file in the file server that is mapped into the clients network drive structure can (and probably will) be corrupted. An example of this kind of malware is the infamous KEYHolder virus.



A much more robust network using a NAS for Disaster Recovery is shown here:



Using a NAS for Disaster Recovery

In the more robust network shown in the diagram, the NAS is not mapped onto the Client network. It is highly desirable that this device is configured to be isolated from the client network. The NAS should not have access to the internet. Given the fact that NAS appliances are very low cost (especially relative to a SAN), the expense should not pose a barrier of entry. Think of the NAS as a very large thumb drive.

Of course, a large number of backup solutions are available. If this were a Windows® environment for instance, one could easily install CrashPlan PROe™ Server on the NAS, and CrashPlan PROe™ Client on the Server, for the nominal cost of a single client license. This would allow multiple restore points from the NAS in case a malicious malware event occurs. As long as there wasn't a catastrophe in the server room, the NAS could have the Server restored in a matter of minutes.

Even if the Server was being protected with nightly offsite backups for disaster recovery purposes, restoring the server from the NAS locally over the intranet would be much faster than over the internet. Also, backing up or restoring the server from the NAS would not impact the performance of the internet or the client network, since it's totally isolated from both.

Of course, as in any good server management, permissions should only be granted to clients that need access to reduce the exposure to malware. As an example, accounting employees won't need access to engineering development files, and vice versa.