Router
Router vermitteln die Daten zwischen zwei oder mehreren Subnetzen, die beispielsweise durch Weitverkehrsleitungen wie ISDN verbunden sind. Auch ein Einsatz im LAN ist möglich, um die Datensicherheit zu erhöhen.
Wenn es darum geht, mehrere Rechner ins Internet zu bringen, gibt es zwei Lösungen. Die eine, jedem Rechner ein Modem und eine Einwählverbindung zu spendieren, kostet allein durch die Telefongebühren eine ganze Menge Geld. Komfortabler und billiger geht es, wenn sich nur einer der Rechner ins Internet einwählt und die anderen über diesen Rechner auf das Web zugreifen. Dieser zentrale Rechner wird im Allgemeinen als Gateway oder Router bezeichnet.

Routing bezeichnet das Weiterleiten von Netzwerk-Paketen. Ein TCP/IP-Paket findet seinen Weg über eine Anzahl von Routern, die das Paket über ein Netzwerk-Device eintgegennehmen und anhand ihrer Routing-Tabelle entscheiden, welchen Weg das Paket weiter nehmen soll.

Proxy
Meist als Kurzform für Proxy-Cache verwendet. Dabei handelt es sich um eine Komponente des Proxy-Servers einer Firewall. Der Cache speichert beispielsweise Internetseiten lokal zwischen, sodass sie beim nächsten Abruf nicht vom Internetserver geholt werden müssen, sondern schneller und kostengünstiger aus dem lokalen Cache.
Proxies wurden entwickelt, um WWW-Zugriffe zu beschleunigen. Ein Proxy arbeitet generell wie ein Cache-Speicher in einem Computer. Wird eine Seite von einem Browser angefordert, wird zuerst der Proxy befragt, ob er diese Seite in seinem lokalen Speicher vorrätig hat, damit die meist teuren und überfüllten Fernleitungen nicht belastet werden. Einen solchen Mechanismus haben wir auch auf unserem Wohnheimserver eingerichtet. In diesem Proxy werden nur Seiten vorrätig gehalten, die nicht älter als zwei Tage sind. Der Inhalt des Proxies ist also sehr aktuell. Wir bitten alle Teilnehmer am Wohnheim-Netzwerk darum, den Proxy zu benutzen, da damit unsere Verbindung zum Rechenzentrum der TU, die nur eine Bandbreite von 2 Mbit/s hat, extrem entlastet werden kann, denn viele Anfragen können lokal beantwortet werden.

Firewall
Mit Firewalls lassen sich Netzwerke gegen unbefugte Zugriffe von außen absichern. Die verfügbaren Lösungen reichen von der Zusatzsoftware bis hin zu speziellen Geräten, die ausschließlich auf diese Aufgabe ausgelegt sind. In ihrer grundlegenden Funktionsweise unterscheiden sich die Systeme allerdings nur wenig.

Definition einer Firewall
Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz, wie zum Beispiel dem Internet. An dieser "Brandschutzmauer" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind. Damit eine Firewall effektiv arbeiten kann muss entsprechend der gesamte Datenverkehr zwischen dem privaten Netz und dem Internet über diese Station laufen. Die Firewall untersucht alle Pakete und lässt nur die unverdächtigen passieren.

Gateway
Ein Gateway hat nicht nur die Hardware, um 2 Netze zusammenzubinden. Nein, ein Gateway hat auch noch die nötige Software um alle 7 Layer des ISO/OSI-Modells zu verstehen.
Somit ist ein Gateway protokollunabhängig!
Ein Gateway kann somit zum Beispiel ein IPX/SPX Netz mit einem TCP/IP Netz verbinden. Ebenso könnten dann diese IPX/SPX Hosts auf HTTP oder FTP Ports eines TCP/IP Hosts zugreiffen. Der Gateway wandelt die HTTP und FTP Formate in IPX/SPX kompatible um.
Ein weiteres Einsatzgebiet ist die zentrale Datenverarbeitung.
Eine SQL Datenbank auf einem TCP/IP orienterten Server kann so auch vom Macintoshs mit AppleTalk angesprochen werden.
Der Gateway wandelt das AppleTalk in TCP/IP um und stellt auch eine Schnittstelle für SQL Abfragen zur Verfügung.

Was benötigt man zur Absicherung
Als erstes einen Proxy-Server mit Firewall (evtl. Hardwarefirewall in größeren Unternehmen), auf jede Station kann noch eine Softwarefirewall installiert werden. Wichtig sind außerdem die Rechtevergaben, somit kann ein von außen Eindringender nicht soviel Schaden anrichten (wenn man nicht als Admin angemeldet ist). Des weiteren Passwortschutz und Verschlüsselung. Eine Antivirensoftware ist auch von nöten, gute Firewalls und auch Antivirensoftware erkennen außerdem Trojaner.