Proxy Environments

Many districts use **proxy servers** in their network environments. A proxy server sits between client applications, such as a web browser, and a real server. They forward requests from internal nodes to the Internet. Proxy servers can use the these functions to control related actions:

- Protocol filtering - filters protocols that are forwarded to the Internet
- User authentication - controls users that can access the Internet
- Machine authentication - controls workstations that can access the Internet
- Content filtering - filters Internet content users can access
- Content caching - speeds up access for frequently visited sites

For an application to access the Internet in a proxy server environment, the application must know the hostname and port number of the proxy server. The application sends all requests for network services to the proxy server for processing. The proxy server receives the requests and determines what to do with them. If a district implements all functions above, the proxy server verifies that:

- The protocol of the request is serviceable (for example - ICMP, UDP, may be blocked by the proxy server).
- The user authenticates, if the proxy server does not recognize the user login.
- The request source address is on the list of allowed workstations.
- The requested network object is not blocked by an Internet content filter.
  Most Internet content filter vendors provide lists of sites that administrators can decide to block or allow.
- Whether the requested object is cached on the proxy server’s local disk.
  If the object is in cache, the proxy server sends it directly to the requestor without having to access it from the Internet.

If the request passes all verifications above, the proxy server stores a record of the request and issues its own request for the same object to the Internet. When the reply returns to the proxy server, the server matches the reply to the original request stored and forwards the reply to the original requestor.