Introduction to Network Operating Systems

Networks

This document is intended to provide a broad overview of the infrastructure within which a networking operating system functions. It provides a frame of reference, and introduces terminology, important in any discussion of networks, including the relevant operating systems.

Introduction to Networks

A network is a collection of computers, called hosts which can communicate with each other and share resources\(^1\). As a rule, a network is defined by its address, or set of address, about which we will say more later. Such networks are called Local Area Networks (LANs) as the hosts connected to the network are not usually very far from one another (see the lower left section of Figure 1.)

An internetwork (or internet, for short) is a 'network of networks' (Figure 1 shows an example of an Internetwork); that is a number of LANs which can communicate with each other. Of course, we are primarily interested in the Internet,\(^2\) a particular instance of an internetwork which includes the World Wide Web.

Some other terminology used to refer to networks with different geographical scopes are MANs (Metropolitan Area Networks) which typically might be spread over an entire city, and WANs (Wide Area Networks) which may be country-wide or even global. The Internet is frequently considered a WAN.

Networks are further classified with respect to 'who's the boss', so to speak. In peer-to-peer networks all hosts are equal. They share their resources without regard to any one or more of them having special status. Home networks containing Windows hosts are typically peer-to-peer networks. In Client/Server networks, one (or more) of the hosts is designated to provide some service to the other hosts. The host(s) which provide the services are called Servers. Clients make requests of servers while servers respond to these requests. At any point in time, a specific physical host may be either a Client, a Server, or both, depending on the applications being run on the machine.

\(^1\)These resources might belong to one of the hosts, or might themselves be directly connected to the network as if they were hosts. Printers, for example.

\(^2\)Note the uppercase 'I'.

nos_text_intro.wpd
NTC 7/12/05
Components of a Network

Hardware Components

LANs consist of a set of hosts, connected by some communication media, called links. The media may be physical (including twisted-pair wire, coaxial cable, or optical fiber) or wireless. In addition, there may be other Connection Devices such as repeaters, hubs, switches or routers which facilitate connecting the hosts in different environments and/or topologies. The Internet typically connects LANs through the use of a large number of routers, for instance.

Some hosts play special roles in LANs and The Internet. In Figure 1, any host might, at some point in time, be a client (Hc) or a server (Hs) depending on the software running.
Hosts which connect LANs to the Internet are often called **Gateways (Hg in Figure 1)**, Proxy Servers, or Routers.

**Software Components**

In addition to the operating systems running on the hosts, a large number of other programs are needed to allow two hosts to communicate over the network. The purpose of these programs is to implement, in software, the set of **protocols** that allow this communication.

A **protocol** is a *set of rules* that allows two hosts (or other network-connected devices) to communicate with each other. Network devices may be very different in terms of operating systems, data representation, or other characteristics, and network protocols specify what each device needs to do to understand the other. The protocols are implemented by software programs such as HTTP, FTP, SMTP, TCP, etc. depending on the network communication task to be performed.

One of the most important tasks of a protocol is to specify how devices are identified; that is, how they are **addressed**. There are several addressing mechanisms implemented by different protocols, including addressing at the hardware level to identify physical hardware devices (used by ARP), at the host level to uniquely identify a host on the Internet (used by IP), and at the process level to uniquely identify a specific application on a particular host.

Protocols may also specify whether or not communication is **reliable** and, if so, the mechanisms to be used to detect errors and recover from them.

Finally, there are those software components which actually initiate communication across a network, **client software**, or respond to communication initiated elsewhere, **server software**.

Client software are those **applications** which are network-aware and can initiate requests to other hosts. Web browsers, for instance are client applications which request web pages from a web site; e-mail clients request mail be downloaded from a mail server or send mail to a mail server. Server software are those applications which respond to client requests. Web servers, mail servers, and ftp servers are some examples of such software.

Finally, there are a set of software **utilities** which are useful in measuring various network characteristics. These utilities can test connections (**ping**) identify a route from one host to another (**traceroute**), measure performance, etc.