Appendix A
Protocols

The LAN environment of the netWorks application focuses on modeling broadcast network architectures within a single autonomous system (or routing domain), and therefore its protocol requirements are necessarily reduced.

Most computer networks and networking software are architected using a hierarchical model with each layer offering service to the layer built on top of it. Machines connected to the network logically communicate to each other on a layer-to-layer basis (that is, layer 5 of machine 1 communicates to layer 5 of machine 2) using layer specific protocols. A protocol is a predefined set of rules, formats, and conventions that machines agree to follow when attempting to carry on a conversation.

Two common network architectures are the OSI Reference Model and the TCP/IP Reference Model. (See Figure A.1.)

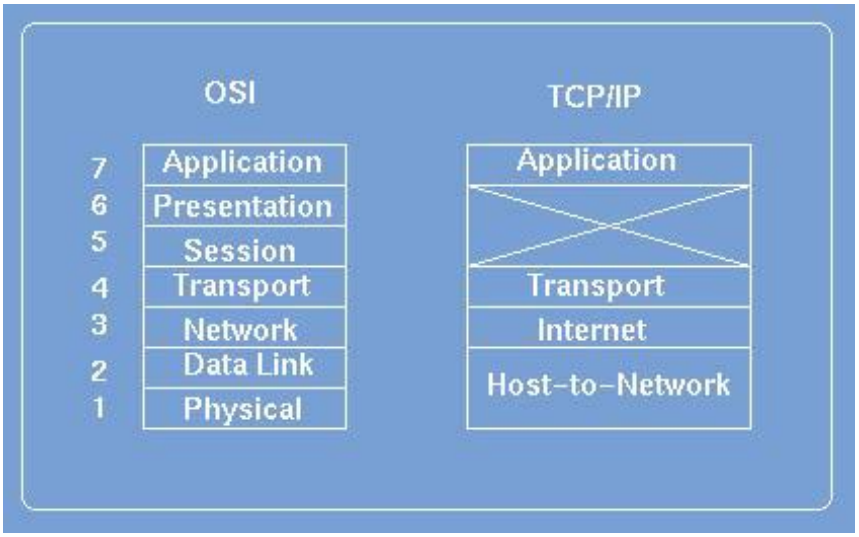

Figure A.1. Reference Models

The details of these reference models can be found in [Tanenbaum 1996] and [Perlman 1992]. The netWorks application provides simulations for some of the protocols used in the data link/host-to-network layers and the Network/Internet layers.

Data Link Layer

The data link layer is responsible for transmitting packets of information across the link between hosts. If the link is shared by many hosts (for example, a LAN) this layer also specifies how access to the media link is controlled. A sublayer of the

data link layer, called the medium access control (MAC) sublayer, addresses access issues.

Addresses

Since every station on the LAN listens to every packet transmission, it needs some means of determining not only which packets are meant for it but also what station sent the packet. Therefore, each network interface card (NIC) is given an address, and each packet contains a destination address and a source address. The IEEE 802 committee, which is responsible for defining the MAC protocols, came up with standardized addresses for its LANs. Most NICs are assigned a 48-bit address at the time of manufacture, but you have the option of changing the default address.

In the netWorks application, an unique integer address is assigned to each NIC model at the time of its instantiation. You cannot change this value.

MAC Protocols

The MAC sublayer offers many different protocols for sharing a transmission medium, but the netWorks application focuses on three MAC protocols defined by the IEEE 802 committee. These protocols are

- 802.3 - CSMA/CD (carrier sense multiple access with collision detection) LAN, derived from Ethernet
- 802.4 - Token Bus LAN
- 802.5 - 4 MB and 16 MB Token Ring LAN

The details for these and other MAC protocols can be found in [Tanembaum 1996] and [Perlman 1992]. A brief overview of each of these protocols is presented in the following sections.

802.3

This IEEE standard defines a carrier-sense, multiple access with collision detection (CSMA/CD) protocol for a bus topology. This is the technology used by Ethernet. A bus topology is depicted in Figure A.2.

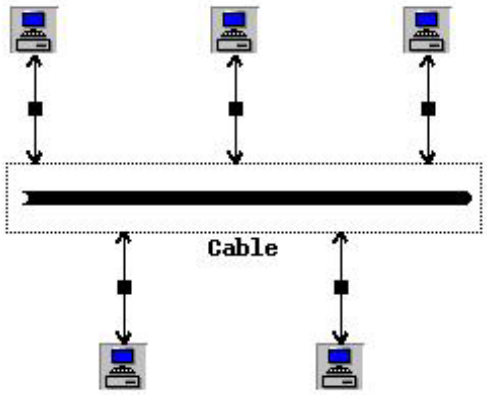

Figure A.2. LAN Bus Topology

When a station on a CSMA/CD LAN wants to transmit a data packet onto the LAN, it first *listens* to see if there is any traffic on the LAN, that is, if anybody else is currently transmitting. If the LAN is available, the station proceeds to broadcast its data packets on to the LAN. All stations attached to the LAN read every packet transmitted on it but they process only the packets addressed to them. If the station detects traffic when it wants to transmit, it waits until the LAN is not busy.

It is possible for two (or more) stations to think the LAN is not busy and both begin transmitting data onto the LAN. This results in a packet collision. The stations running this protocol detect this collision and then reattempt to transmit their data after waiting for a (random) period of time.

There are several variants of the 802.3 standard, each designed for a different transmission media. These include

- 10Base2 - 10 Mbps over thin coaxial cable
- 10Base5 - 10 Mbps over thick coaxial cable
- 10Base-T - 10 Mbps over twisted pair cable
- 10Base-F - 10 Mbps over fiber optic cable
- 100Base-T - 100 Mbps over twisted pair cable

802.4

The 802.4 IEEE standard defines the Token Bus protocol for a token-passing access method on a bus topology. In a token-passing access method, a special packet called a token is passed from station to station and only the token holder is permitted to transmit packets onto the LAN. Thus, no collisions can occur with this protocol. When a station is done transmitting its packets, it passes the token to the "next" station. The next station does not need to be physically closest to this one on the bus,

just the next logical station. A station can hold the token for only a certain amount of time before it must pass it on—even if it has not completed transmitting all of its data. This assures access to all stations on the bus within a specified period of time.

802.5

The 802.5 IEEE standard defines the Token Ring protocol which, like Token Bus, is another token-passing access method, but for a ring topology. A ring topology consists of a series of individual point-to-point links that form a circle. (See Figure A.3.)

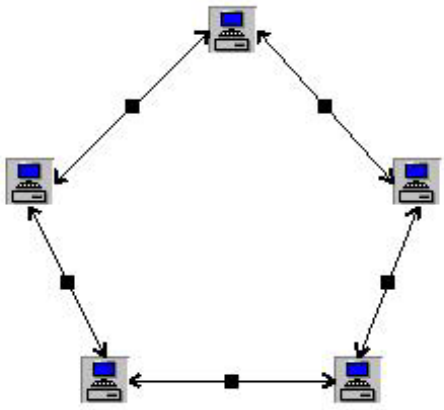

Figure A.3. LAN Ring Topology

A token is passed from station to station in one direction around the ring, and only the station holding the token can transmit packets onto the ring. Data packets travel in only one direction around the ring. When a station receives a packet addressed to it, it copies the packet and puts it back on the ring. When the originating station receives the packet, it removes the packet.

Network Layer

The network layer is responsible for ensuring that every pair of hosts on the network can communicate with each other. It is the lowest layer in the reference models that deals with end-to-end transmission. If the hosts are on separate LANs, this involves finding a path for the data packets through intermediate nodes. To perform this task, the network layer must possess knowledge of the entire network topology; therefore, the equipment on the network must somehow exchange network layer identification information, typically the network addresses. This information is exchanged using neighbor greeting protocols and routing protocols. Neighbor greeting protocols are used by devices on the same LAN to exchange network layer information, while routing protocols are concerned with messages between routers and their associated routing algorithms. A specific neighbor greeting protocol is typically paired in a network

with a particular routing protocol. The netWorks application provides simulations of two protocols for each of these categories.

Network Addresses

As with the MAC sublayer, devices need to determine what packets are destined for them and where they came from. However, routing in the network layer is often hierarchical. In other words, the network may be divided into pieces or subnetworks, so network addresses must accommodate the feature. In a network address, a portion of the address is used to designate the subnetwork and another portion identifies a particular station in that subnetwork. The two most common forms of network addresses are those defined by ISO and the IP protocol.

IP Address

An IP network address is 4 octets (32 bits) long with the left-most bits defining the subnetwork part of the address and the remaining bits defining the host or station portion. The number of bits for each portion is not fixed, so an IP address must be accompanied by a *mask* that specifies the subnetwork segment of the address. An IP address is typically displayed by using a decimal value for each of the octets, separated by periods. The associated mask is sometimes represented in the same format, or it may just be shown as a decimal value for the number of bits to be used for the network portion of the address. Figure A.4 shows the different formats.

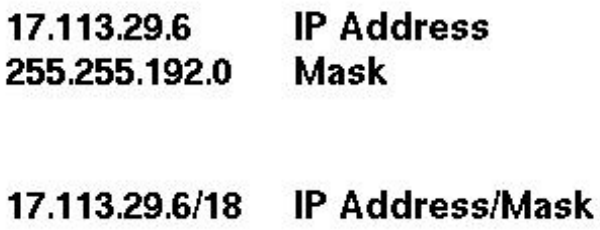

Figure A.4. Sample IP Addresses

In the netWorks application, IP addresses are specified as four integers separated by periods, and masks specify how many of the integers to use for the network portion of the address. Therefore, a mask has a value of either 1, 2, or 3.

ISO Address

ISO network layer addresses are a bit more complex than IP addresses. These addresses are variable length and can be up to 20 octets long. Any packet containing an ISO network layer address must also have a corresponding field with the address' length. The format for an ISO address is displayed in Figure A.5.

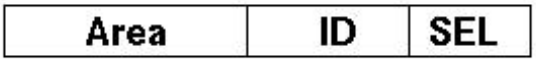

Figure A.5. ISO Address Format

The **AREA** part of the address identifies the level 1 subnetwork or *area*, and the **ID** section identifies the station in the area. The **AREA** portion of an ISO network address actually can be divided into subfields with each specifying a different level subnet in a hierarchical routing scheme. (The notion of areas is discussed in the Routing Protocols section.) The **SEL** section of the address is used to differentiate different network layer users.

The netWorks application takes a simpler approach to ISO addresses, and its ISO address format is shown in Figure A.6. ISO network addresses are specified in netWorks as three integers, separated by periods.

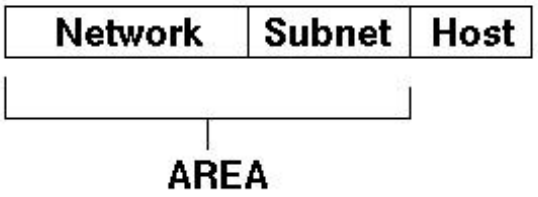

Figure A.6. netWorks ISO Address Format

Neighbor Greeting Protocols

Neighbor greeting protocols are used to find data link and network layer addresses of other devices on the same LAN—including adjacent routers. This information is exchanged by transmitting special packets or messages between stations attached to a LAN. Stations store any information collected in local storage called caches. When a station needs to transmit data packets to another station, it looks in its cache for the address of the destination and, if found, places the address information in the data packets and sends them on their way. Different protocols have different algorithms for handling the case in which the destination information is not in the cache. The cache is usually purged periodically to remove outdated information.

As mentioned previously, a specific neighbor greeting protocol is typically deployed in conjunction with a particular routing protocol. The netWorks application contains simulations of the End System - Intermediate System (ES-IS) neighbor greeting protocol specified in ISO document ISO/IEC 9542 and the Address Resolution Protocol (ARP) defined in RFC 826. These protocols are used in conjunction with the IS-IS and OSPF routing protocols, respectively. The following sections provide a brief overview of the ES-IS and ARP protocols. The protocol details can be found in [Perlman 1992].

ES-IS

End systems running ES-IS periodically transmit *end-system hello* packets onto the LAN, thereby announcing their presence to other systems. Similarly, intermediate systems (routers) periodically broadcast *intermediate-system hello* packets onto the LAN. The stations listen to these messages and populate their caches based on the information contained in the hello packets. Note that this protocol is generating traffic on the LAN whether or not any data packets need to be transmitted. This protocol is fully defined in [ISO/IEC-9542].

ARP

The ARP protocol takes a different approach from ES-IS to acquiring neighbor information. Instead of sending periodic hello packets, the ARP protocol populates its cache on an "as needed" basis. If an end system running ARP wants to send data packets to another destination and that destination's address information is not found in its local cache, the end system tries to determine whether the destination is on the same LAN as itself. If the destination is on the same LAN, the end system broadcasts an ARP query packet onto the LAN seeking the destination's address information. The destination sends a response packet back to the original end system with the requested information, and the original end system updates its cache and transmits the data packets. If the destination is on a different LAN, the transmitting end system sends the data packets to a router on the LAN and lets it forward the packets.

There are different implementations of ARP for end stations to determine what routers are attached to the LAN. In some cases, an end system might be manually configured with a router address; in others, end systems listen for routing protocol packets and then extract router information from them.

This protocol is defined in [Plummer 1982].

Routing Protocols

Network layer routing protocols provide the communication protocols and algorithms for determining routes to every destination and also for distributing the routing information throughout the network. Routing protocols are categorized as either interior (intradomain) or exterior (interdomain) routing protocols, with interior protocols designed to work only within a domain or autonomous system. An algorithm that is efficient at intradomain routing might not be well-suited for interdomain routing. The LAN subsystem of netWorks provides simulations for several interior routing protocols designed for broadcast networks.

All popular routing protocols are based on one of the following distributed algorithms:

- Distance Vector
- Link State

The first routing protocols employed distance vector routing. In this scheme each router keeps track of the distance to each of its neighbors and then transmits this vector to every neighbor. The routers then use the set of all distance vectors they receive to determine the shortest paths to each destination.

In link state algorithms, routers determine their neighbors (and the cost to each) by exchanging hello packets. They then construct link state packets containing a list of their neighbors (and associated costs) and flood these packets throughout the entire domain. Using the link state packets, the routers can construct a graph of the network and then calculate the "best" paths through it. Link state algorithms converge more quickly than distance vector algorithms, but this typically require more memory and CPU processing than distance vector algorithms.

The netWorks application provides simulations of two link state protocols:

- Intermediate System - Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

Both of these protocols use the notion of hierarchical routing to reduce the amount of link state information the routers need to exchange. In hierarchical routing, the network is subdivided into separate, logical units typically called *areas*, and routers share their link state information with other routers in their area. Some routers have additional responsibilities to forward packets between areas. These are considered to be at a higher level in the hierarchical routing scheme, and the routing protocol defines separate procedures for forwarding packets within an area versus between areas.

The IS-IS and OSPF protocols both elect a Designated Router (DR) on LANs with more than one router attached to them. The protocols typically use the router's priority and router ID in the DR selection process. The DR is responsible for collecting and distributing the link state information for all the routers on its LAN throughout its area. This helps reduce the protocol traffic on the network. In the OSPF routing protocol, a Backup Designated Router (BDR) is also elected to take over should the DR fail.

The following sections provide a brief overview of the IS-IS and OSPF routing protocols.

IS-IS

The IS-IS routing protocol is a link state protocol for interior routing. It is an ISO standard and is completely defined in [ISO/IEC-10589]. The ES-IS neighbor greeting

protocol is used in conjunction with IS-IS. For its hierarchical routing, IS-IS divides the network into nonoverlapping IS-IS areas and its routers are categorized as Level 1 or Level 2 routers, or both. Level 1 routers are responsible for routing packets between LANs within an IS-IS area, and Level 2 routers forward packets between IS-IS areas. A sample IS-IS topology is depicted in Figure A.7.

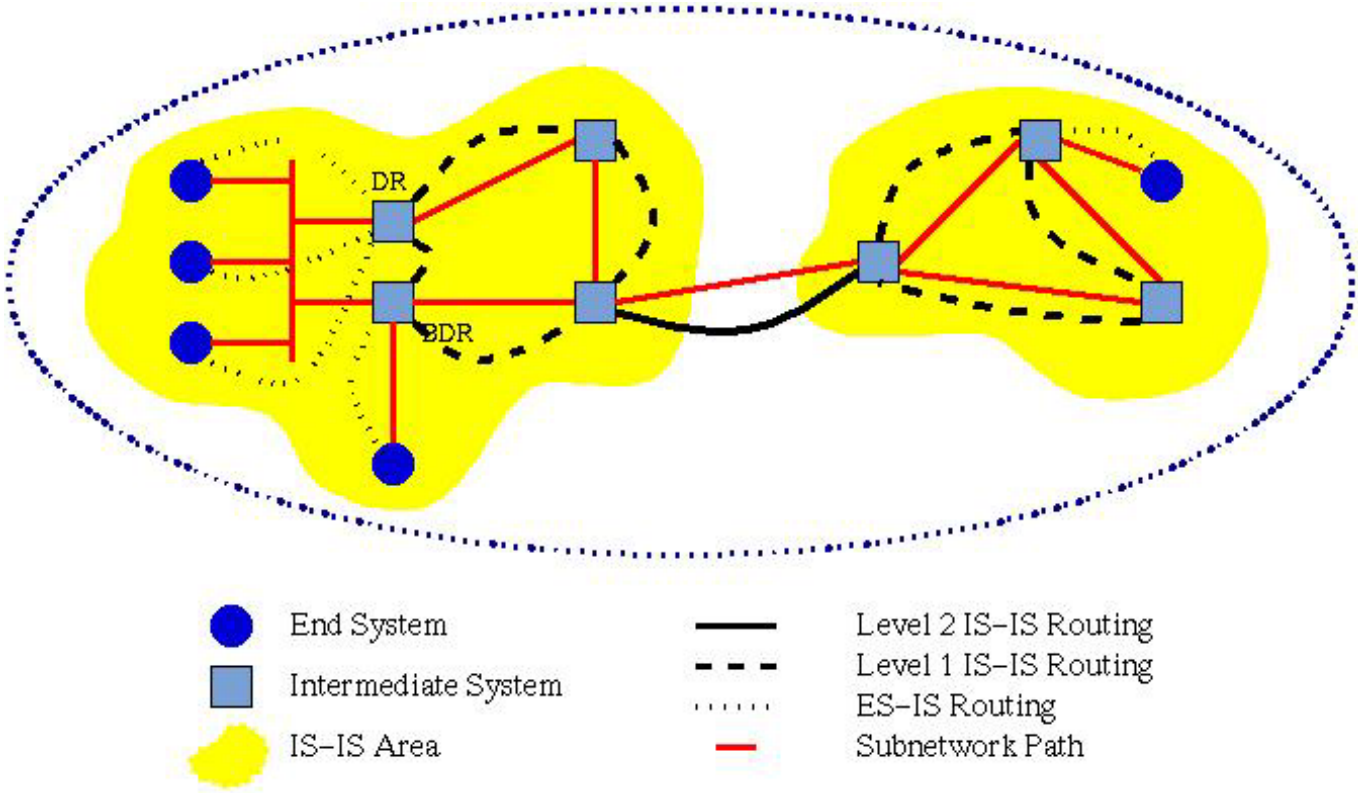

Figure A.7. Sample IS-IS Topology

In the IS-IS routing protocol, Level 1 routers transmit Level 1 hello packets to the other Level 1 routers on the LANs to which they are connected. Level 2 routers operate in a similar manner. (Note that a LAN may actually be a point-to-point connection between two routers.) The routers collect and process all of their neighbor routers hello packets and populate a local cache with the state of all its router links. Each router (or DR for a LAN) periodically floods its link state information to all other routers at its level in a Link State packet. The routers use all the link state information to create a graph of the network. From this graph, the router is able to determine the "best" path for forwarding packets it receives; that is, the router creates a table (or forwarding database) stating which port to use to transmit packets towards their destination. The basic algorithm used for route calculation is the *shortest path first* algorithm invented by Dijkstra and described in [Aho 1983]. Routers periodically recalculate their routing tables to reflect any new link state information. A Level 1 router recognizes the fact that a data packet is destined for another IS-IS area and forwards the packet to a Level 2 router for inter-Area routing.

The netWorks simulation of the IS-IS routing protocol does not support Level 2 routing at this time.

The IS-IS protocol provides a number of configurable parameters that can be tuned for your particular network model. The IS-IS control panel for a Router model, shown in Figure A.8, displays the protocol parameters you can change in the netWorks version of IS-IS. You should be fairly familiar with the internals of the IS-IS protocol before you edit these fields. Note that units for the Timing Intervals are milliseconds.

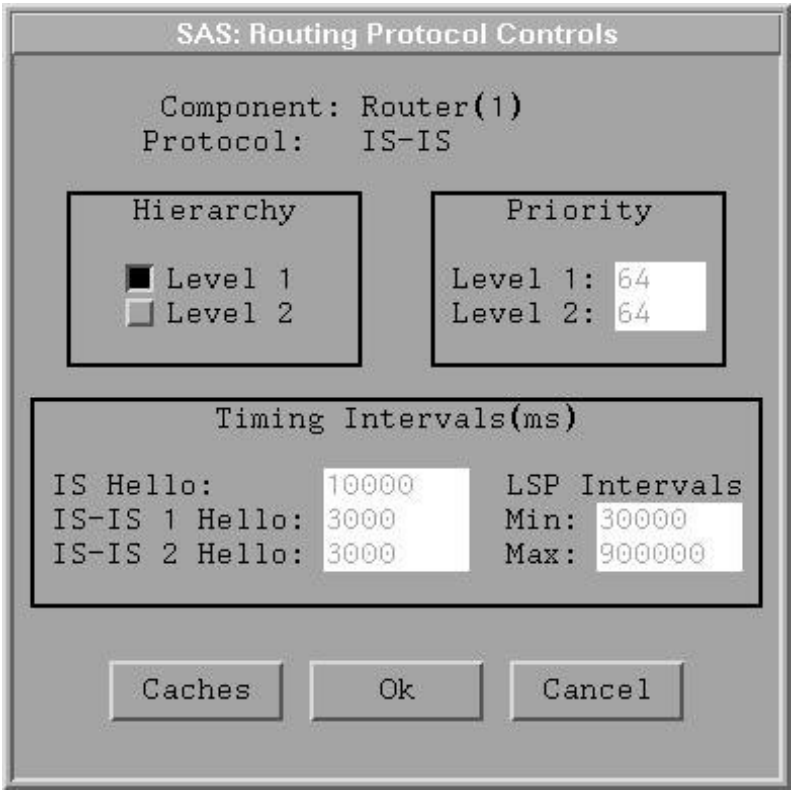

Figure A.8. Sample IS-IS Protocol Controls

OSPF

The Open Shortest Path First (OSPF) routing protocol is another link state protocol for interior routing. It was developed by the Internet Engineering Task Force specifically for the TCP/IP internet environment. OSPF was designed after IS-IS, and since it borrowed a lot of ideas from the IS-IS routing protocol, the two protocols have many similarities. A complete description of OSPF can be found in RFC 2178 [Moy 1997] and [Moy 1998].

OSPF also divides the network into areas; however, OSPF has a special area (Area 0) called the OSPF backbone. The backbone distributes routing information between non-backbone areas. Unlike the IS-IS protocol, a router can be part of two or more

different areas in OSPF. These routers are called *area border routers*, and their functionality is similar to the Level 2 routers in IS-IS. An area border router runs a separate copy of the basic OSPF algorithm for each area to which it belongs. A sample OSPF topology is depicted in Figure A.9.

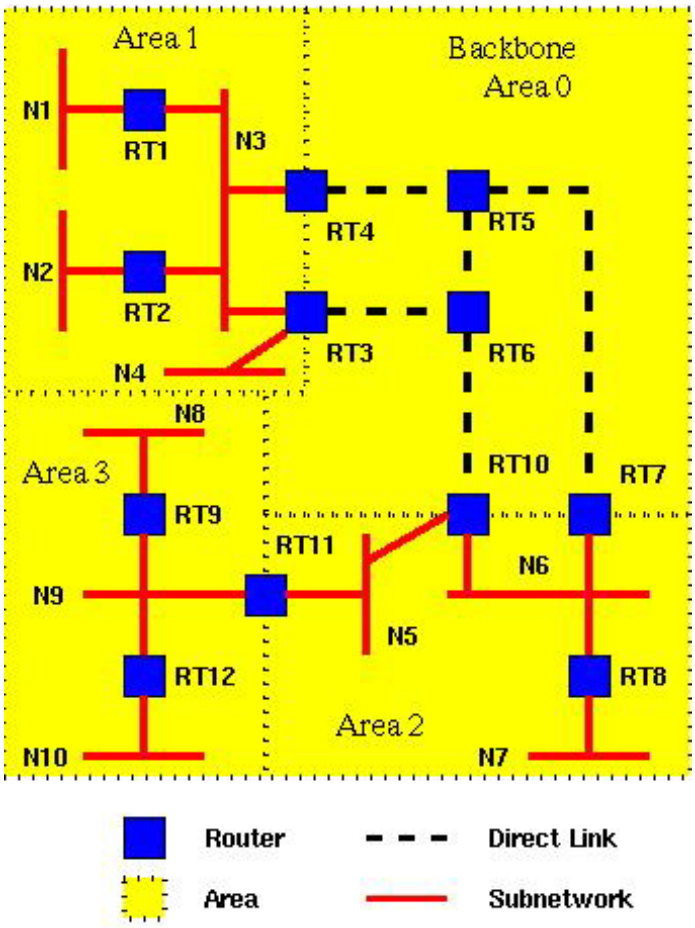

Figure A.9. Sample OSPF Topology

This sample network domain has 4 areas, each with multiple LANS and routers. Routers RT3 and RT4 are examples of area border routers, while routers RT1 and RT2 are referred to as *internal routers*. The backbone routers in this example include RT5 and RT6 as well as RT3, RT4, RT7, and RT10.

As in IS-IS, OSPF routers periodically transmit hello packets and keep an internal database with information from all neighbor hellos they receive. When a router gets a hello packet from another router, a Designated Router (DR) is elected (if they are on the same LAN) and an attempt is made to form what is called an adjacency. For two routers to become fully adjacent, they must first establish two-way communication between them and synchronize their link state databases. Adjacencies can be established only when one of the routers is the DR or BDR or when the connection between the routers is a point-to-point link.

Each router periodically floods link information packets called *link state advertize-*

The correct bibliographic citation for this manual is as follows: SAS Institute Inc., *SAS/OR Software: The netWorks Application, Version 8*, Cary, NC: SAS Institute Inc., 1999. 89 pp.

SAS/OR Software: The netWorks Application, Version 8

ISBN 1-58025-487-X

SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

1st printing, October 1999

The Institute is a private company devoted to the support and further development of its software and related services.