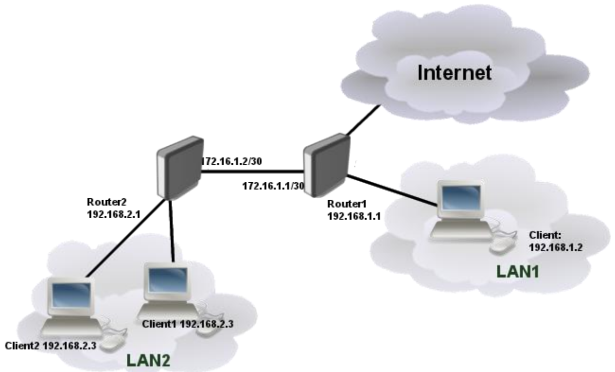


# ROUTING PROTOCOLS

Dorian Stefan Sengher
Victor Botan

**Network**

# Routing

**Routing** is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. However, that latter function is better described as forwarding. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

In case of overlapping/equal routes, algorithms consider the following elements to decide which routes to install into the routing table (sorted by priority):

1. *Prefix-Length*: where longer subnet masks are preferred (independent of whether it is within a routing protocol or over different routing protocol)
2. *Metric*: where a lower metric/cost is preferred (only valid within one and the same routing protocol)
3. *Administrative distance*: where a route learned from a more reliable routing protocol is preferred (only valid between different routing protocols)

# Routing Protocols

In the two decades since their invention, the heterogeneity of networks has expanded further with the deployment of Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, Switched Multimegabit Data Service (SMDS), Integrated Services Digital Network (ISDN), and most recently, Asynchronous Transfer Mode (ATM). The Internet protocols are the best proven approach to internetworking this diverse range of LAN and WAN technologies.

The Internet Protocol suite includes not only lower-level specifications, such as Transmission Control Protocol (TCP) and Internet Protocol (IP), but specifications for such common applications as electronic mail, terminal emulation, and file transfer. Figure 1 shows the TCP/IP protocol suite in relation to the OSI Reference model. Figure 2 shows some of the important Internet protocols and their relationship to the OSI Reference Model. For information on the OSI Reference model and the role of each layer, please refer to the document Internetworking Basics.

The Internet protocols are the most widely implemented multivendor protocol suite in use today. Support for at least part of the Internet Protocol suite is available from virtually every computer vendor.

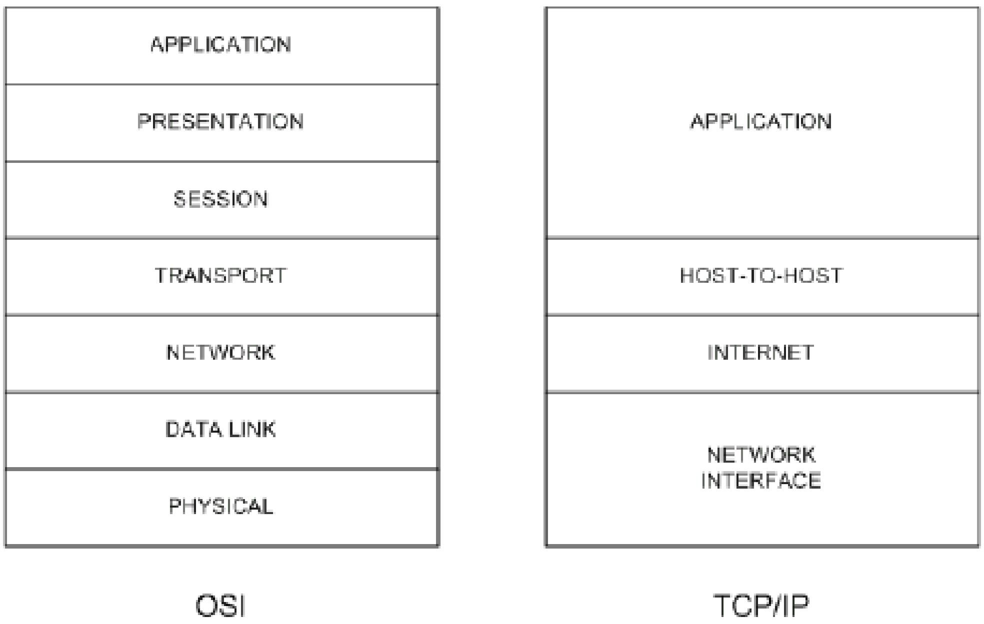


***Figure 1***

# RIP v2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all Must Be Zero protocol fields in the RIPv1 messages are properly specified. In addition, a compatibility switch feature] allows fine-grained interoperability adjustments.

In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

(MD5) authentication for RIP was introduced in 1997.

RIPv2 is Internet Standard STD56 (which is RFC 2453).

Route tags were also added in RIP version 2. This functionality allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.

# OSPF(Open Shortest Path First)

OSPF is an interior gateway protocol (IGP) for routing Internet Protocol (IP) packets solely within a single routing domain, such as an autonomous system. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer which routes datagrams based solely on the destination IP address found in IP packets. OSPF supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks and featuresvariable-length subnet masking (VLSM) and Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The OSPF routing policies for constructing a route table are governed by link cost factors (*external metrics*) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), data throughput of a link, or link availability and reliability, expressed as simple unitless numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network may be structured, or subdivided, into routing *areas* to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.

# EIGRP(Enhanced Interior Routing Protocol)

The Enhanced Interior Gateway Routing Protocol is instead of Interior Gateway Routing Protocol (IGRP) in 1993. One of the major reasons for this was because the design of the Internet Protocol had been changed to support classless IPv4 addresses, which IGRP could not support.

Almost all routers contain a routing table that contains rules by which traffic is forwarded in a network. If the router does not contain a valid path to the destination, the traffic is discarded. EIGRP is a dynamic routing protocol by which routers automatically share route information. This eases the workload on a network administrator who does not have to configure changes to the routing table manually.

In addition to the routing table, EIGRP uses the following tables to store information:

- Neighbor Table: The neighbor table keeps a record of the IP addresses of routers that have a direct physical connection with this router. Routers that are connected to this router indirectly, through another router are not recorded in this table as they are not considered neighbors.
- Topology Table: The topology table stores routes that it has learned from neighbor routing tables. Unlike a routing table, the topology table does not store all routes, but only routes that have been determined by EIGRP. The topology table also records the metrics for each of the listed EIGRP routes, the feasible successor and the successors. Routes in the topology table are marked as

"passive" or "active". Passive indicates that EIGRP has determined the path for the specific route and has finished processing. Active indicates that EIGRP is still trying to calculate the best path for the specific route. Routes in the topology table are not usable by the router until they are inserted into the routing table. The topology table is never used by the router to forward traffic. Routes in the topology table will not be inserted into the routing table if they are active, are a feasible successor, or have a higher administrative distance than an equivalent path.

Information in the topology table may be inserted into the router's routing table and can then be used to forward traffic. If the network changes, for example, a physical link fails or is disconnected, the path will become unavailable. EIGRP is designed to detect these changes and will attempt to find a new path to the destination. The old path that is no longer available is removed from the routing table. Unlike most distance vector routing protocols, EIGRP does not transmit all the data in the router's routing table when a change is made but will only transmit the changes that have been made since the routing table was last updated. EIGRP does not send its routing table periodically, but will only send routing table data when an actual change has occurred. This behavior is more inline with link-state routing protocols, thus EIGRP is mostly considered a hybrid protocol.

When a router running EIGRP is connected to another router also running EIGRP, information is exchanged between the two routers and a relationship is formed known as an adjacency. The entire routing table is exchanged between both routers at this time. After this has occurred, only differential changes are sent.

EIGRP is often considered a hybrid protocol because it is also sends link state updates when link states change.