**What is the difference between routing and forwarding?**  
  
My Name isXXXXX will be helping you today. If I provide good service, you may ask for The-PC-Guy in your question title for your future needs.  
  
It is more complex than the previous answer you recieved.  
  
Routing is when 2 networks are shared by a device usually a router. The way the router works is it maintains an IP adress - mac adress table.   
  
It would look something like this  
  
ip mac  
192.168.1.100 (NNN) NNN-NNNNB  
10.0.0.50 FEDCBA098765  
  
now when mac addressNNN-NN-NNNN.. requests some information from FEDC .... it doesn't know what FEDC... mac address is but it knows what the IP address is.  
  
so what it does is it has a router, and says to the router I want information from 10.0.0.50, the router says hey I have a host with that IP address, here is its MAC adress FEDC.... etc... then the 192.168.1.100 can send the request to 10.0.0.50 through the router. So the router acts sort of like a mediator making sure that requests go to the correct place  
  
Port fowarding is slightly different, every function on a network is assigned a port, common ones, are websites to port 80, ftp to port 21, email on ports 110 and 25 and so on.   
  
Port forwarding can be set up in this way  
  
say I have 2 computers on my network one is a web server the other is ftp server.  
  
web server IP = 192.168.1.100  
ftp server IP = 192.168.1.101  
  
and for exmple my public IP is 100.75.50.25. now when someone types in my IP address without a port the router will not know what to do. So I set up port forwarding which says send all requests for port 80 to 192.168.1.100,   
  
now when someone goes to a browser and types my ip adress 100.75.50.25 my router says hey thats a request for port 80, I am suposed to forward that to 192.168.1.100, and you will see my website. Same thing for ftp with port 21.  
  
Read more: <http://www.justanswer.com/computer/682o2-difference-routing-forwarding.html#ixzz3ovIBEqOX>

**Note:**

1.

Forwarding does not know about where destination is..  
It just just longest prefix and consider as there might be destination.  
  
Where routing is sure that route to specific network and there is destination network. route will be select on different with different protocol.

2.

Routing is determining which way the packet will use to reach its destination easily and effectively, While forwarding refers to when the information enters the router and it defines when it will be sent!

3.

Routing is based on knowing where the destination is and to which interface the layer 3 device should send it to..  
Forwarding on the other hand is just receiving the packet and forwarding it in a hope that it would reach its destination.  
  
Basically routing is where the device knows how to reach the destination whereas forwarding is just forwarding the packet not knowing whether it would reach destination or not..

4.

Routing answers the question of what next hop IP to send a packet based on the destination prefix.  
  
Forwarding functions determine which exit interface to use to send the packet to its next hop.

[APPLICATION LAYER - ROUTING PROTOCOLS](http://www.freesoft.org/CIE/RFC/1812/143.htm)

The Internet routing system consists of two components - interior routing and exterior routing. The concept of an Autonomous System (AS), plays a key role in separating interior from an exterior routing. Autonomous Systems must provide each other with topology information to allow such forwarding. Interior gateway protocols (IGPs) are used to distribute routing information within an AS (i.e., intra-AS routing).

**Routing Security Considerations**

Routing is one of the few places where the **Robustness Principle (be liberal in what you accept) does not apply.** Routers should be relatively suspicious in accepting routing data from other routing systems.

A router SHOULD provide the ability to rank routing information sources from most trustworthy to least trustworthy and to accept routing information about any particular destination from the most trustworthy sources first.

A router SHOULD provide a mechanism to filter out obviously invalid routes.

Routers MUST NOT by default **redistribute routing data** they do not themselves use, trust or otherwise consider valid.( only happen under direct intercession by some human agency.)

Routers must be at least a little paranoid about accepting routing data from anyone.

### Precedence

Except where the specification for a particular routing protocol specifies otherwise, a router SHOULD set the IP Precedence value for IP datagrams carrying routing traffic it originates to 6 (INTERNETWORK CONTROL).

### Message Validation

The application of message passwords and explicit acceptable neighbor lists has in the past improved the robustness of the route database. Routers SHOULD IMPLEMENT management controls that enable explicit listing of valid routing neighbors. Routers SHOULD IMPLEMENT peer-to-peer authentication for those routing protocols that support them.

Routers SHOULD validate routing neighbors **based on their source address and the interface a message is received on**; neighbors in a directly attached subnet SHOULD be restricted to communicate with **the router via the interface that subnet is posited on or via unnumbered interfaces**. Messages received on other interfaces SHOULD be silently discarded.

### 7.2 INTERIOR GATEWAY PROTOCOLS

An Interior Gateway Protocol (IGP) is used to distribute routing information between the various routers in a particular AS.

Independent of the algorithm used to implement a particular IGP, it should perform the following functions:

1. Respond quickly to changes in the **internal topology of an AS**
2. **Provide a mechanism such that circuit flapping does not cause continuous routing updates**
3. **Provide quick convergence to loop-free routing**
4. **Utilize minimal bandwidth**
5. Provide **equal cost routes to enable load**-splitting
6. **Provide a means for authentication of routing updates**

Current IGPs used in the internet today are characterized as either being based on a **distance-vector or a link-state algorithm.**

A router that implements any routing protocol (other than static routes) MUST IMPLEMENT OSPF.

A router MAY implement additional IGPs.

### OPEN SHORTEST PATH FIRST - OSPF

Shortest Path First (SPF) based routing protocols are a class of link-state algorithms that are based on the shortest-path algorithm of Dijkstra. Although SPF based algorithms have been around since the inception of the ARPANET, it is only recently that they have achieved popularity both inside both the IP and the OSI communities. In an SPF based system, each router obtains the entire topology database through a process known as flooding. Flooding insures a reliable transfer of the information. Each router then runs the SPF algorithm on its database to build the IP routing table. The OSPF routing protocol is an implementation of an SPF algorithm.

Note: RFC-1131, which describes OSPF

### INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM - DUAL IS-IS

IS-IS is based on a link-state (SPF) routing algorithm and shares all the advantages for this class of protocols.

### 7.3 EXTERIOR GATEWAY PROTOCOLS

Exterior Gateway Protocols are utilized for inter-Autonomous System routing to exchange reachability information for a set of networks internal to a particular autonomous system to a neighboring autonomous system.

The Border Gateway Protocol (BGP) eliminates many of the restrictions and limitations of EGP, and is therefore growing rapidly in popularity. A router is not required to implement any inter-AS routing protocol. However, if a router does implement EGP it also MUST IMPLEMENT BGP. Although it was not designed as an exterior gateway protocol, RIP is sometimes used for inter-AS routing.

### BORDER GATEWAY PROTOCOL – BGP

### The Border Gateway Protocol (BGP-4) is an inter-AS routing protocol that exchanges network reachability information with other BGP speakers. The information for a network includes the complete list of ASs that traffic must transit to reach that network. This information can then be used to insure loop-free paths. This information is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced.

### One must focus on the rule that an AS advertises to its neighbor ASs only those routes that it itself uses. This rule reflects the hop-by-hop routing paradigm generally used throughout the current Internet. Note that some policies cannot be supported by the hop-by-hop routing paradigm and thus require techniques such as source routing to enforce. For example, BGP does not enable one AS to send traffic to a neighbor AS intending that traffic take a different route from that taken by traffic originating in the neighbor AS. On the other hand, BGP can support any policy conforming to the hop-by-hop routing paradigm.

### Protocol Walk-through

### At a minimum, however, a BGP implementation:

### SHOULD allow an AS to control announcements of the BGP learned routes to adjacent AS's. Implementations SHOULD support such control with at least the granularity of a single network. Implementations SHOULD also support such control with the granularity of an autonomous system, where the autonomous system may be either the autonomous system that originated the route, or the autonomous system that advertised the route to the local system (adjacent autonomous system).

1. SHOULD allow an AS to prefer a particular path to a destination (when more than one path is available). Such function SHOULD be implemented by allowing system administrator to assign weights to Autonomous Systems, and making route selection process to select a route with the lowest weight (where weight of a route is defined as a sum of weights of all AS's in the AS\_PATH path attribute associated with that route).
2. SHOULD allow an AS to ignore routes with certain AS's in the AS\_PATH path attribute. Such function can be implemented by using technique outlined in (2), and by assigning infinity as weights for such AS's. The route selection process must ignore routes that have weight equal to infinity.

### INTER-AS ROUTING WITHOUT AN EXTERIOR PROTOCOL

It is possible to exchange routing information between two autonomous systems or routing domains without using a standard exterior routing protocol between two separate, standard interior routing protocols. The most common way of doing this is to run both interior protocols independently in one of the border routers with an exchange of route information between the two processes.

As with the exchange of information from an EGP to an IGP, without appropriate controls these exchanges of routing information between two IGPs in a single router are subject to creation of routing loops.

### 7.4 STATIC ROUTING

### A router SHOULD provide a means for defining a static route to a destination, where the destination is defined by a network prefix. The mechanism SHOULD also allow for a metric to be specified for each static route.

A router that supports a dynamic routing protocol **MUST allow static routes to be defined with any metric valid for the routing protocol used.** **The router MUST provide the ability for the user to specify a list of static routes that may or may not be propagated through the routing protocol.** In addition, a router SHOULD support the following additional information if it supports a routing protocol that could make use of the information. They are:

* **TOS,**
* **Subnet Mask, or**
* **Prefix Length, or**
* **A metric specific to a given routing protocol that can import the route.**

**Note:**

The ToS field could specify a datagram's priority and request a route for low-delay, high-throughput, or highly-reliable service.

Based on these ToS values, a packet would be placed in a prioritized outgoing queue,[[4]](https://www.wikiwand.com/en/Type_of_service" \l "citenote4) or take a route with appropriate latency, throughput, or reliability

A router MUST allow a metric to be assigned to a static route for each routing domain that it supports. Each such metric MUST be explicitly assigned to a specific routing domain. For example:

route 10.0.0.0/8 via 192.0.2.3 rip metric 3

route 10.21.0.0/16 via 192.0.2.4 ospf inter-area metric 27

route 10.22.0.0/16 via 192.0.2.5 egp 123 metric 99

**Note:**

It has been suggested that, ideally, static routes should have preference values rather than metrics (since metrics can only be compared with metrics of other routes in the same routing domain, the metric of a static route could only be compared with metrics of other static routes). **This is contrary to some current implementations, where static routes really do have metrics, and those metrics are used to determine whether a particular dynamic route overrides the static route to the same destination. ++**

**This technique essentially makes the static route into a RIP route, or an OSPF route (or whatever, depending on the domain of the metric). Thus, the route lookup algorithm of that domain applies.**

For static routes not put into a **specific routing domain, the route lookup algorithm is:**

1. **Basic match**
2. **Longest match**
3. **Weak TOS (if TOS supported)**
4. **Best metric (where metric are implementation-defined)**

### 7.5 FILTERING OF ROUTING INFORMATION

Each router within a network makes forwarding decisions based upon information contained within its forwarding database. In a simple network the contents of the database may be configured statically. **As the network grows more complex, the need for dynamic updating of the forwarding database becomes critical to the efficient operation of the network.**

### If the data flow through a network is to be as efficient as possible, it is necessary to provide a mechanism for controlling the propagation of the information a router uses to build its forwarding database.

This control takes the form of choosing which sources of routing information should be trusted and selecting which pieces of the information to believe. The resulting forwarding database is a filtered version of the available routing information.

In addition to efficiency, controlling the propagation of routing information can reduce instability by preventing the spread of incorrect or bad routing information.

### Route Validation

A router SHOULD log as an error any routing update advertising a route that violates the specifications of this memo, unless the routing protocol from which **the update was received uses those values to encode special routes (such as default routes).**

### Basic Route Filtering

Filtering of routing information allows control of paths used by a router to forward packets it receives. A router should be selective in which sources of routing information it listens to and what routes it believes. **Therefore, a router MUST provide the ability to specify:**

* **On which logical interfaces routing information will be accepted and which routes will be accepted from each logical interface.**
* **Whether all routes or only a default route is advertised on a logical interface.**

Some routing protocols do not recognize logical interfaces as a source of routing information. In such cases the router MUST provide the ability to specify

* From which other routers routing information will be accepted.

For example, assume a router connecting one or more leaf networks to the main portion or backbone of a larger network. Since each of the leaf networks has only one path in and out, the router can simply send a default route to them. It advertises the leaf networks to the main network.

### Advanced Route Filtering

As the topology of a network grows more complex, the need for more complex route filtering arises.

Therefore, a router SHOULD provide the ability to specify independently for each routing protocol:

* Which logical interfaces or routers routing information (routes) will be accepted from and which routes will be believed from each other router or logical interface,
* Which routes will be sent via which logical interface(s), and
* Which routers routing information will be sent to, if this is supported by the routing protocol in use.

In many situations it is desirable to assign a reliability ordering to routing information received from another router instead of the simple believe or don't believe choice listed in the first bullet above. A router MAY provide the ability to specify:

* A reliability or preference to be assigned to each route received. A route with higher reliability will be chosen over one with lower reliability regardless of the routing metric associated with each route.

If a router supports assignment of preferences, the router MUST NOT propagate any routes it does not prefer as first party information. **If the routing protocol being used to propagate the routes does not support distinguishing between first and third party information, the router MUST NOT propagate any routes it does not prefer**.

*For example, assume a router receives a route to network C from router R and a route to the same network from router S. If router R is considered more reliable than router S traffic destined for network C will be forwarded to router R regardless of the route received from router S.*

Routing information for routes which the router does not use (router S in the above example) MUST NOT be passed to any other router.

### 7.6 INTER-ROUTING-PROTOCOL INFORMATION EXCHANGE

**Routers MUST be able to exchange routing information between separate IP interior routing protocols, if independent IP routing processes can run in the same router.** Routers MUST provide some mechanism for avoiding routing loops when routers are configured for bi-directional exchange of routing information between two separate interior routing processes. **Routers MUST provide some priority mechanism for choosing routes from independent routing processes.** Routers SHOULD provide administrative control of IGP-IGP exchange when used across administrative boundaries.

**Routers SHOULD provide some mechanism for translating or transforming metrics on a per network basis.** Routers (or routing protocols) **MAY allow for global preference of exterior routes imported into an IGP.**

**Note:**

Different IGPs use different metrics, requiring some translation technique when introducing information from one protocol into another protocol with a different form of metric. Some IGPs can run multiple instances within the same router or set of routers. In this case metric information can be preserved exactly or translated.

There are at least two techniques for translation between different routing processes. The static (or reachability) approach uses the existence of a route advertisement in one IGP to generate a route advertisement in the other IGP with a given metric. The translation or tabular approach uses the metric in one IGP to create a metric in the other IGP through use of either a function (such as adding a constant) or a table lookup.

Bi-directional exchange of routing information is dangerous without control mechanisms to limit feedback. This is the same problem that distance vector routing protocols must address with the split horizon technique and that EGP addresses with the third-party rule. Routing loops can be avoided explicitly through use of tables or lists of permitted/denied routes or implicitly through use of a split horizon rule, a no-third-party rule, or a route tagging mechanism. Vendors are encouraged to use implicit techniques where possible to make administration easier for network operators.