# I341 - TCP/IP ROUTING PROTOCOLS

***Rev: 2016***

## Introduction:

Routing is the process of determining where to send data packets destined for addresses outside of the local network (subnet). Routers gather and maintain routing information to enable the transmission and receipt of such data packets. Routing information is maintained as entries in a routing table, with one entry for each identified route. The router can create and maintain the routing table dynamically to accommodate network changes wherever they occur.

## Interior and Exterior Gateway Protocols:

The term **gateway** is used when discussing routing protocols, when referring to a router. Gateway in ISO (OSI model) terms has the implications of doing full seven layer translation between two separate architecture devices i.e. SNA to DECnet, Apollo Domain to TCP/IP. In terms of interconnecting TCP/IP networks the term gateway infers that a particular router has different interfaces residing on two totally separate IP networks (not existing within the same subnetted network).

Two gateways (routers) within an autonomous system are called **interior**. Two gateways (routers) exchanging routing information are called **exterior,** if they belong to different autonomous systems.

## Interior Gateway Protocols:

Interior Gateway Protocols are used for routing within networks under a common network administration (autonomous system). They include:

RIP (Routing Information Protocol) - developed at Berkeley
Hello (RFC)
OSPF (Open Shortest Path First)
IGRP (Interior Gateway Routing Protocol) - cisco
EIGRP Enhanced IGRP (cisco)

**Exterior Gateway Protocols**:

Exterior Gateway protocols are used for routing networks not under a common network administration (autonomous system). They include:

EGP (Exterior Gateway Protocol)
BGP (Border Gateway Protocol) - BGP4 (BGP Ver4 now prevalent with ISPs)

**Autonomous Systems**:

All routers belonging to a particular autonomous system number indicated in the router by a decimal number (up to 16 bits available) will exchange routing tables.

**Routing (Static versus Dynamic):**

Static Routing:  done by manually adding routes to particular interfaces.

Dynamic Routing: adjusts in real time to changing network conditions.

**Routing Algorithm Metrics:**

segment with the highest bandwidth
accumulated delay
smallest MTU (Max size transmission unit)
reliability
load
hops (number of hops)
cost (of a hop - an admin. metric assigned by LAN designer/engineer)

## Routing Algorithms

### RIP:

Rip is a distance vector protocol designed by Xerox, to be used in PUP (Xerox PARC Universal Protocol).  Rip has been widely adopted by many computer vendors. AppleTalk uses a modified version of RIP in its RTMP (Routing Table Maintenance Protocol), as does Novell IPX.  RIP is used to find neighboring routers.  RIP was designed long ago (1980) and thus worked fine in small homogeneous type networks. RIP is limited to 16 hops max, and cannot choose routes based on real time changes in the network.

**RIP (cont.):**

RIP works well for small isolated and simple topology networks. It uses broadcast UDP (User Datagram Protocol) data packets to exchange routing information. Each router sends router information updates every 30 seconds, in a process referred to as route advertising. If a router doesn't receive an update from another router for 90 seconds, it marks the router by router (not update) as being unusable. If still no update occurs after 240 seconds, the router removes all routing table entries for the non-updating router.

The metric that RIP uses to rate value of the different routes is hop count. Hop count indicated the number of routers that can be traversed in a route (maximum 16 hops). RIP Limitations - RIP lacked metric sophistication, hop count limit and bandwidth impact.

**IGRP:**

IGRP is a proprietary protocol based on distance vector routing. It allows load balancing; line sharing using delay, bandwidth, reliability and MTU in calculating routing decisions. Each router basically only maintains knowledge of its neighbor and which path it takes to get there (thru which interface). Routing tables are exchanged/updated every 30 seconds based on parameters set up in the router installation.

Cisco developed IGRP (Interior G/W Routing Protocol) for routing in an autonomous system containing complex topologies and media with diverse bandwidth and delay characteristics. IGRP advertises all connected networks for a particular autonomous system.

**Router Syntax**

Router IGRP XXX (autonomous system #)
Network (all networks directly connected to the router)

example:

```
router  IGRP 100
network  193.74.237.0
network  193.74.238.0
network  193.74.239.0
```

IGRP uses several types of metric information in making routing decisions. For **each** path through an autonomous system, IGRP records the segment with the lowest bandwidth, the accumulated delay, smallest MTU maximum transmission unit, the reliability and load.

IGRP metric is a 32 bit quantity that is a sum of segment delays and the lowest segment bandwidth for a given route. If a network were comprised of all homogeneous media, this would translate to a hop count. For networks of mixed media (FDDI, Ether, Token Ring, Serial-9600 Bps to T1 and T3) the route with the lowest metric indicates the most desirable path to a destination.

**IGRP Updates**

A router sends an IGRP broadcast update every 90 seconds. IGRP will declare a route inaccessible if it does not receive an update from the first router in the route within 3 update periods (270 sec.). After 7 router update periods the router will remove the route from the routing table.

**OSPF (Open Shortest Path First):**

OSPF is a link state protocol developed for IP networks by the IETF (Internet Engineering Task Force.). Basically information about attached router interfaces, metrics used and other variables are included in OSPF routing updates. This information is flooded throughout the routing area. As OSPF routers accumulate link state information, they are able to calculate the shortest path to each node. "Hello" messages act as keepalives to let routers know other routers are still functional. Updates are only required when a link state changes. Additional OSPF features include multi-path routing state changes. Additional OSPF features include multi-path routing (load balancing) and ability to prioritize traffic based on urgency.

OSPF distributes routing information between routers belonging to a single autonomous system. OSPF is a departure from the traditional IP routing protocols such as RIP and IGRP, which utilize distance vector technologies. OSPF (Version 2) protocol is documented in the Internet RFC 1247.

**OSPF Router Classifications:**

Internal Router - within an area
Area Border Router - between areas
Backbone Router - backbone is always area 0 (must be contiguous). Does not touch any other areas
Area System Boundary Router - Serves as boundary to router "talking" to external autonomous systems.

OSPF uses the Hello protocol, which is periodically sent out through all router interfaces. Bi-directional communication is indicated when the router sees itself listed in the neighbors Hello packet.

## BGP

BGP (Border Gateway Protocol) is a recently developed exterior routing protocol that resolves some of the inherent problems of EGP. It is implemented on a wide scale basis, especially by Internet Service Providers (ISPs).

## Principle of Operation for Distance Vector & Link State Protocols

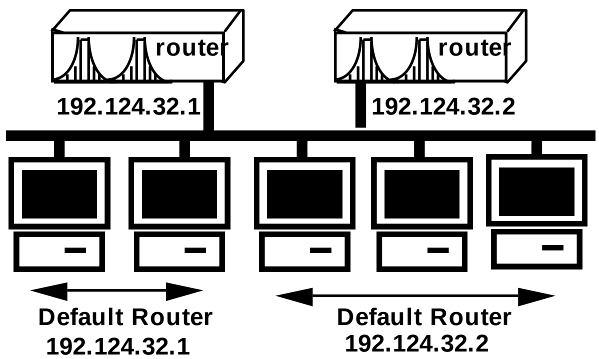
**Distance Vector:** In distance vector routing, each router exchanges information with its neighboring (adjacent) routers to advertise distances (metric cost) to known destinations (IP addresses). Each router computes its own distance to a destination by examining the neighbor's advertised cost and adding the cost of the link to that neighbor. If the calculated result causes a router to alter its route, as determined by minimizing the cost to each destination, then the router informs its neighbors. The procedure converges when no router changes its routes upon receipt of routing updates from its neighbors. Once convergence is achieved, routers periodically update neighbors regarding the cost to destinations.

**Distance Vector & Link State Protocols (cont.):**

**Link State**: In link state routing, each router broadcasts to all other routers (within a defined routing domain) the distance (metric cost) to each of its neighboring (adjacent) routers using a Link State Packet (LSP). Each router can thereby build a complete topology map of the routing domain and individually compute routes, by using a path minimization algorithm (e.g. Dijkstara SPF) to achieve convergence. LSP's are generated periodically or with a change in the state of a link or addition of a new neighbor.

In LSPs, the types of metrics used to calculate destination include: cost, bandwidth, delay, load, and reliability). Internet scalability is a function of the specific IGP (i.e. an internet of a given size may be an issue of scale for one IGP but not for another).

**Host Router Discovery Protocol (RDP)**




The TCP/IP host (end system) configurations examined in class all contain a parameter called default router (or default gateway). This points to the device that would provide services if IP datagrams need to be forwarded off the network. If there were two routers on a segment/subnet for redundancy (or a subnet containing mission critical servers), if one of the routers failed then the default router statement contained in one of the groups of stations (see above illustration) would not permit IP datagrams to go off net without configuring each IP host to point to the correct (alive/functioning) default router.

Solution: some IP hosts have a capability called Router Discovery Protocol (more prevalent in UNIX systems) that eliminates the default router/gateway statement. Instead by turning on RDP, they listen for router broadcasts (the routers pick one primary router) and continue to use that router/path until some event (router failure - no broadcast) occurs.

**Using Static Routes (instead of Dynamic) in a Router**

Routers that use the same routing protocol (IGP, OSPF, RIP) will dynamically "learn" about other routers **speaking the same routing protocol** on the network. In the illustration below, the AppleTalk LocalTalk network devices are running TCP/IP and AppleTalk protocols. AppleTalk routers typically do not know any routing protocol but RIP and for reasons (we hopefully have learned from the sections above) we do not wish to turn on a hop based, hop limited (15 hops), no sophisticated metrics or consideration of available bandwidth, network load etc....

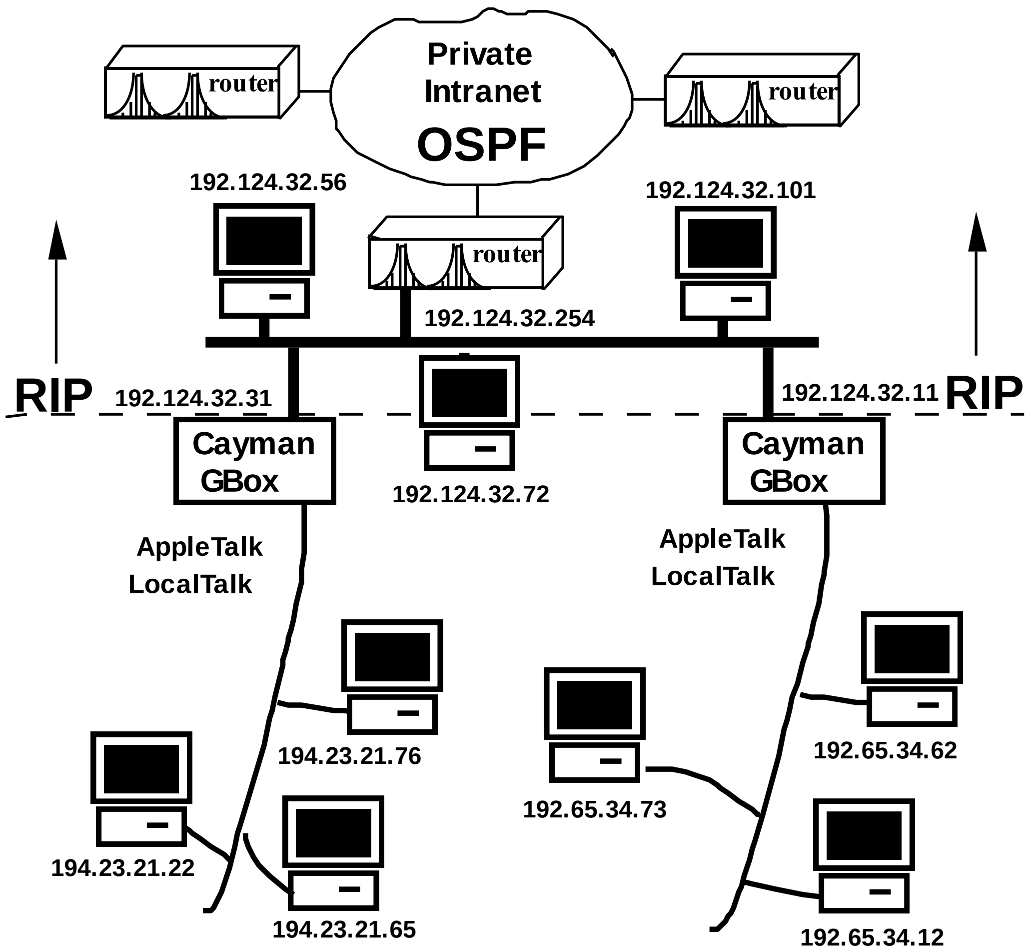
**Problem**: AppleTalk Routers speak RIP, routers connecting all locations over the companies private intranet all use OSPF as their routing protocol.

**Solution**: Use static routes in the OSPF routers to "see" the LocalTalk networks. Once the OSPF (local) router learns about these networks (by seeing the static entries in the routing table - it will include the networks in routing table updates to OSPF partners (if told to do so).

Router Configuration: (using static routes) to support illustrated network below

IP route 192.65.34.0 192.124.32.11
IP route 194.23.21.0 192.124.32.31

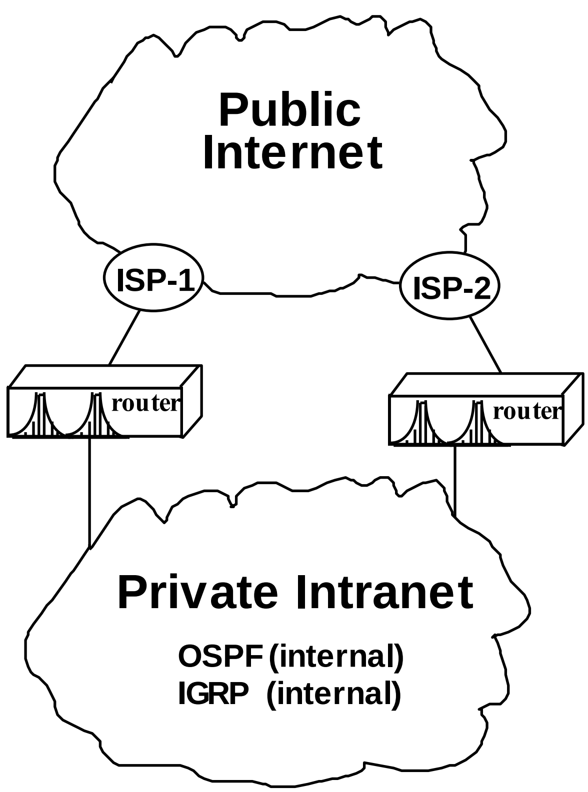
**BE CAREFUL** using Static Routes – Failure to remove static routes and their lack of flexibility during outages/failures makes them **VERY DANGEROUS** if not kept under strict controls.




Routing Protocol Figure – Static Route Example 1

**BGP**

The Border Gateway Protocol (BGP), defined in RFC 1771, allows you to create loop free inter-domain routing between autonomous systems. An autonomous system is a set of routers under a single technical administration. Routers in an AS can use multiple interior gateway protocols to exchange routing information inside the AS and an exterior gateway protocol to route packets outside the AS. BGP is an inter-Autonomous System (AS) routing protocol. The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS and using an exterior gateway protocol to route packets to other autonomous systems. It is common for a single AS to use several interior gateway protocols. The network reachability information exchanged via BGP provides sufficient information to detect routing loops and enforce routing decisions based on performance preference and policy constraints as outlined in RFC 1104. BGP exchanges routing information containing full AS paths and enforces routing policies based on configuration information. BGP-4 is an extension of BGP-3 that provides support for routing information aggregation and reduction based on the Classless inter-domain routing architecture (CIDR), and will be the version of BGP tested for deployment. One of BGP's greatest attributes is the ability to provide alternate routing thru Public and Private Networks - using dual ISPs. The following illustration depicts how BGP would be utilized in dual ISP environment.



## BGP Operation

BGP uses TCP as its transport protocol (port 179). Two BGP speaking routers form a TCP connection between one another (peer routers) and exchange messages to open and confirm the connection parameters.  BGP routers will exchange network reachability information, this information is mainly an indication of the full paths (BGP AS numbers) that a route should take in order to reach the destination network. This information will help in constructing a graph of ASs that are loop free and where routing policies can be applied in order to enforce some restrictions on the routing behavior.

## Peers (BGP Neighbors)

Any two routers that have formed a TCP connection in order to exchange BGP routing information, are called BGP peers, they are also called BGP neighbors.

## Information Exchange Between Peers

BGP peers will initially exchange their full BGP routing tables. From then on incremental updates are sent as the routing table changes. BGP keeps a version number of the BGP table and it should be the same for all of its BGP peers. The version number will change whenever BGP updates the table due to some routing information changes. Keep-alive packets are sent to ensure that the connection is alive between the BGP peers and notification packets are sent in response to errors or special conditions.