Interior and Exterior Gateway Protocol Concepts

Interior Gateway Protocols (IGPs) manage routing within a single network or Autonomous System (AS), while Exterior Gateway Protocols (EGPs) handle routing between different ASs, enabling broader internet connectivity.

Here's a more detailed explanation:

Interior Gateway Protocols (IGPs):

- **Scope:**

  IGPs operate within a single Autonomous System (AS), which is a group of routers under common administration with common routing policies.

- **Purpose:**

  They facilitate data routing within the boundaries of that AS, optimizing the delivery of packets between routers within the same network.

- **Examples:**
- **RIP (Routing Information Protocol):** An older, simpler protocol that uses hop count as a metric.
- **OSPF (Open Shortest Path First):** A more modern protocol that uses **link-state technology** for faster convergence.
- **EIGRP (Enhanced Interior Gateway Routing Protocol):** A Cisco-proprietary protocol that combines features of distance-vector and link-state protocols.
- **Internal Routers:**

  Routers within an AS that connect only to other routers in the same AS run IGPs.

Exterior Gateway Protocols (EGPs):

- **Scope:**

  EGPs operate between different Autonomous Systems (ASs).

- **Purpose:**

  They enable communication and data exchange between networks managed by different organizations or entities.

- **Examples:**

- **BGP (Border Gateway Protocol):** The de facto standard inter-domain routing protocol used in the Internet.
- **Border Routers:**

  Routers that connect an AS to other ASs (or the internet) run both IGPs and EGPs.

- **EGP vs BGP:**
  While the original EGP was used for inter-domain routing, BGP has largely replaced it as the dominant protocol for this purpose.

Open Shortest Path First

Open Shortest Path First (OSPF) is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP).

In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates.

An LSA is a packet that contains information about neighbors and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm.

In the context of Open Shortest Path First (OSPF) routing, a Link-State Advertisement (LSA) is a **message** that routers use to share information about their local network topology, including their connected links and associated costs, with other routers in the same OSPF area.

OSPF has the following key advantages:

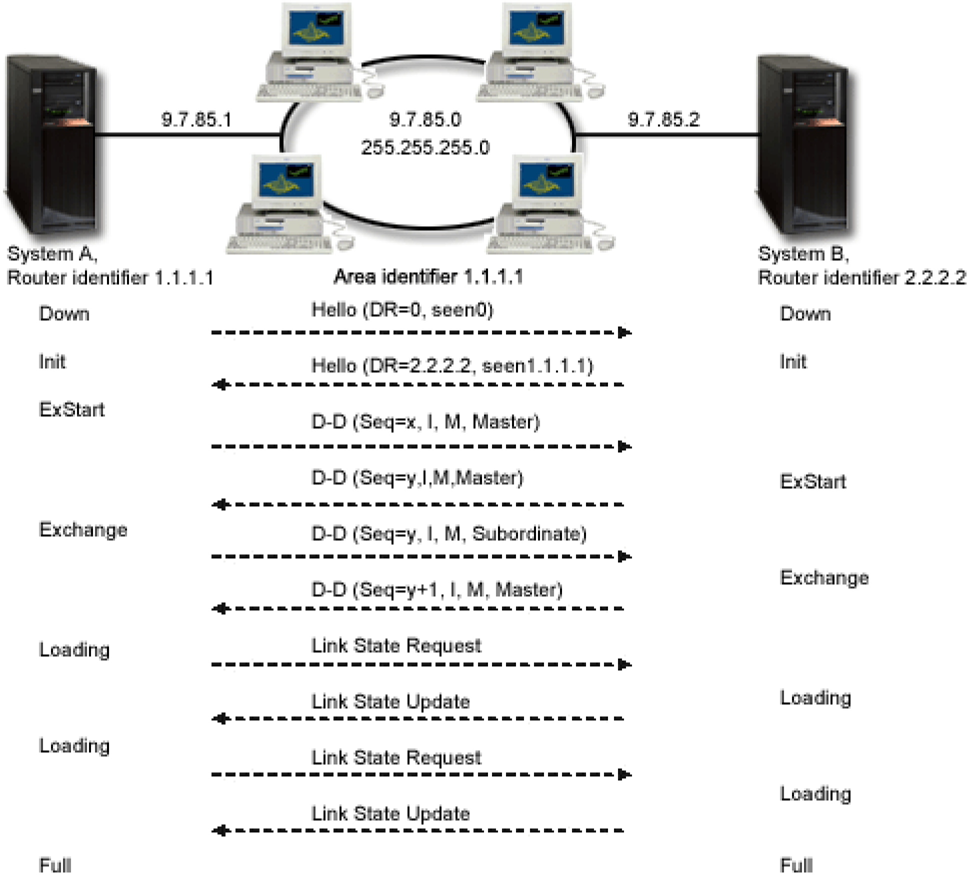
- Compared with distance-vector routing protocols such as the Routing Information Protocol (RIP), OSPF is more suitable for serving large, heterogeneous internetworks. OSPF can recalculate the routes in a short amount of time when the network topology changes.
- With OSPF, you can divide an Autonomous System (AS) into areas and keep area topologies separate to decrease the OSPF routing traffic and the size of the link-state database of each area.
- OSPF provides equal-cost multipath routing. You can add duplicate routes to the TCP stack using different next hops.

OSPF Hello protocol and link-state database exchange

After routers or systems in an OSPF network ensure that their interfaces are functional, they first send out Hello packets, using the Hello protocol over their OSPF interfaces, to discover neighbors. Neighbors are routers or systems that have interfaces to the common network. After that, neighboring routers or systems exchange their link-state databases to establish adjacencies.

The following figure illustrates the process of discovering neighbors and establishing adjacencies for two systems in the 9.7.85.0 subnet. Each system has an OSPF interface to the common subnet 9.7.85.0 (interface 9.7.85.1 for system A and interface 9.7.85.2 for system B). Subnet 9.7.85.0 belongs to area 1.1.1.1.

Figure 1. OSPF Hello protocol and database exchange



EXSTART phase

This is the first step of the link-state database exchange. The two systems negotiate who is the master and who is the subordinate.

EXCHANGE phase

The two systems exchange Database Description packets to find out the LSAs that the link-state database of each system does not include. Each system stores the LSAs that are not included in its link-state database in the retransmission list.

LOADING phase

Each system sends Link State Request packets to request the neighbor (the other system in this example) to send to it the entire LSAs that were stored in the retransmission list during the EXCHANGE phase. The neighbor responds to the request with the LSAs in Link State Update packets.

FULL phase

When the two systems finish exchanging LSAs and their link-state databases are synchronized, adjacency is established between the two systems.

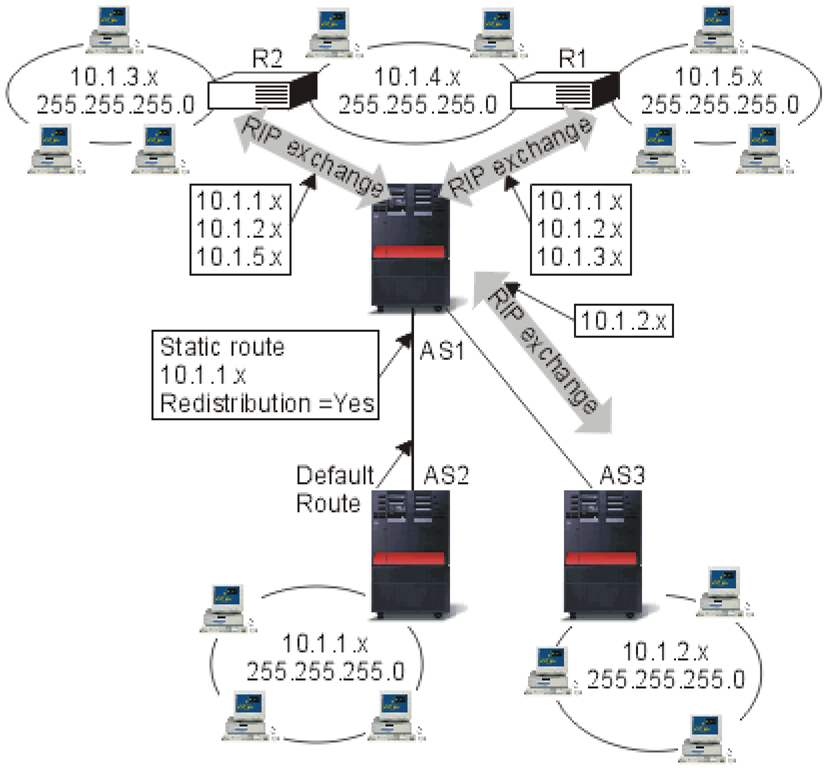
After adjacencies are established between all the routers or systems in an area, each router or system in the area periodically sends an LSA to share its adjacencies or to report its state change. By comparing the established adjacencies with the LSAs, routers or systems in the area can discover the area topology changes and update their link-state databases accordingly.

Routing Information Protocol

Routing Information Protocol (RIP) is a distance-vector routing protocol. Routers running the distance-vector protocol send all or a portion of their routing tables in routing-update messages to their neighbors.

You can use RIP to configure the hosts as part of a RIP network. This type of routing requires little maintenance and also automatically reconfigures routing tables when your network changes or network communication stops. RIPv2 was added to the IBM® i product so you can send and receive RIP packets to update routes throughout your network.

In the following figure, a static route is added to the central system (AS1) that describes the connection to the network 10.1.1.x by way of AS2. This is a static route (added by your network administrator) with route redistribution set to yes. This setting causes this route to be shared with other routers and systems so that when they have traffic for 10.1.1.x, they route the traffic to your central IBM i platform (AS1). AS2 has the routed system started so that it sends and receives RIP information. In this example, AS1 is sending the message that AS2 has a direct connection to 10.1.2.x.



The following process describes the routing of traffic in the preceding figure.

- AS1 receives this RIP packet from AS2 and processes it. If AS1 does not have a route to 10.1.2.x, it will store this route. If it does have a path to 10.1.2.x that is the same number of hops or fewer, it will discard this new route information. In this example, AS1 keeps the route data.
- AS1 receives information from R1 with route information to 10.1.5.x. AS1 keeps this route information.
- AS1 receives information from R2 with route information to 10.1.3.x. AS1 keeps this route information.
- The next time AS1 sends RIP messages, it will send information to R1 that describes all the connections AS1 knows about that R1 might not know about. AS1 sends route information about 10.1.1.x, 10.1.2.x, and 10.1.3.x. AS1 does not send information about 10.1.4.x to R1 because AS1 knows that R1 is connected to 10.1.4.x and does not need a route. Similar information is sent to R2 and AS3.

What is BGP?

Border Gateway Protocol (BGP) is the postal service of the Internet. When someone drops a letter into a mailbox, the Postal Service processes that piece of mail and chooses a fast, efficient route to deliver that letter to its recipient. Similarly, when someone submits data via the Internet, BGP is responsible for looking at all of the available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

BGP is the protocol that makes the Internet work by enabling data routing. When a user in Singapore loads a website with origin servers in Argentina, BGP is the protocol that enables that communication to happen quickly and efficiently.

What is an autonomous system?

The Internet is a network of networks. It is broken up into hundreds of thousands of smaller networks known as autonomous systems (ASes). Each of these networks is essentially a large pool of routers run by a single organization.

If we continue to think of BGP as the Postal Service of the Internet, ASes are like individual post office branches. A town may have hundreds of mailboxes, but the mail in those boxes must go through the local postal branch before being routed to another destination. The internal routers within an AS are like mailboxes. They forward their outbound transmissions to the AS, which then uses BGP routing to get these transmissions to their destinations.

The diagram above illustrates a simplified version of BGP. In this version there are only six ASes on the Internet. If AS1 needs to route a packet to AS3, it has two different options:

Hopping to AS2 and then to AS3:

AS2 → AS3

Or hopping to AS6, then to AS5, AS4, and finally to AS3:

AS6 → AS5 → AS4 → AS3

In this simplified model, the decision seems straightforward. The AS2 route requires fewer hops than the AS6 route, and therefore it is the quickest, most efficient route. Now imagine that there are hundreds of thousands of ASes and that hop count is only one part of a complex route selection algorithm. That is the reality of BGP routing on the Internet.

The structure of the Internet is constantly changing, with new systems popping up and existing systems becoming unavailable. Because of this, every AS must be kept up to date with information regarding new routes as well as obsolete routes. This is done through peering sessions where each AS connects to neighboring ASes with a TCP/IP connection for the purpose of sharing routing information. Using this information, each AS is equipped to properly route outbound data transmissions coming from within.

Here is where part of our analogy falls apart. Unlike post office branches, autonomous systems are not all part of the same organization. In fact, they often belong to competing businesses. For this reason, BGP routes sometimes take business considerations into account. ASes often charge each other to carry traffic across their networks, and the price of access can be factored into which route is ultimately selected.

What is the difference between external BGP and internal BGP?

Routes are exchanged and traffic is transmitted over the Internet using external BGP (eBGP). Autonomous systems can also use an internal version of BGP to route through their internal networks, which is known as internal BGP (iBGP). It should be noted that using internal BGP is NOT a requirement for using external BGP. Autonomous systems can choose from a number of internal protocols to connect the routers on their internal network.

External BGP is like international shipping. There are certain standards and guidelines that need to be followed when shipping a piece of mail internationally. Once that piece of mail reaches its destination country, it has to go through the destination country’s local mail service to reach its final destination. Each country has its own internal mail service that does not necessarily follow the same guidelines as those of other countries. Similarly, each autonomous system can have its own internal routing protocol for routing data within its own network.

What is tunneling?

In the physical world, tunneling is a way to cross terrain or boundaries that could not normally be crossed. Similarly, in networking, tunnels are a method for transporting data across a network using protocols that are not supported by that network. Tunneling works by encapsulating packets: wrapping packets inside of other packets. (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)

Tunneling is often used in virtual private networks (VPNs). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

How does packet encapsulation work?

Data traveling over a network is divided into packets. A typical packet has two parts: the header, which indicates the packet's destination and which protocol it uses, and the payload, which is the packet's actual contents.

An encapsulated packet is essentially a packet inside another packet. In an encapsulated packet, the header and payload of the first packet goes inside the payload section of the surrounding packet. The original packet itself becomes the payload.

Why is encapsulation useful?

All packets use networking protocols — standardized ways of formatting data — to get to their destinations. However, not all networks support all protocols. Imagine a company wants to set up a wide area network (WAN) connecting Office A and Office B. The company uses the IPv6 protocol, which is the latest version of the Internet Protocol (IP), but there is a network between Office A and Office B that only supports IPv4. By encapsulating their IPv6 packets inside IPv4 packets, the company can continue to use IPv6 while still sending data directly between the offices.

Encapsulation is also useful for encrypted network connections. *Encryption* is the process of scrambling data in such a way that it can only be unscrambled using a secret encryption key; the process of undoing encryption is called *decryption*. If a packet is completely encrypted, including the header, then network routers will not be able to forward the packet to its destination since they do not have the key and cannot see its header. By wrapping the encrypted packet inside another unencrypted packet, the packet can travel across networks like normal.

What is a VPN tunnel?

A VPN is a secure, encrypted connection over a publicly shared network. Tunneling is the process by which VPN packets reach their intended destination, which is typically a private network.

Many VPNs use the IPsec protocol suite. IPsec is a group of protocols that run directly on top of IP at the network layer. Network traffic in an IPsec tunnel is fully encrypted, but it is decrypted once it reaches either the network or the user device. (IPsec also has a mode called "transport mode" that does not create a tunnel.)

Another protocol in common use for VPNs is Transport Layer Security (TLS). This protocol operates at either layer 6 or layer 7 of the OSI model depending on how the model is interpreted. TLS is sometimes called SSL (Secure Sockets Layer), although SSL refers to an older protocol that is no longer in use.

What is split tunneling?

Usually, when a user connects their device to a VPN, all their network traffic goes through the VPN tunnel. Split tunneling allows some traffic to go outside of the VPN tunnel. In essence, split tunneling lets user devices connect to two networks simultaneously: one public and one private.

What is GRE tunneling?

Generic Routing Encapsulation (GRE) is one of several tunneling protocols. GRE encapsulates data packets that use one routing protocol inside the packets of another protocol. GRE is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks.

GRE adds two headers to each packet: the GRE header and an IP header. The GRE header indicates the protocol type used by the encapsulated packet. The IP header encapsulates the original packet's IP header and payload. Only the routers at each end of the GRE tunnel will reference the original, non-GRE IP header.

What is IP-in-IP?

IP-in-IP is a tunneling protocol for encapsulating IP packets inside other IP packets. IP-in-IP does not encrypt packets and is not used for VPNs. Its main use is setting up network routes that would not normally be available.

What is SSH tunneling?

The Secure Shell (SSH) protocol sets up encrypted connections between client and server, and can also be used to set up a secure tunnel. SSH operates at layer 7 of the OSI model, the application layer. By contrast, IPsec, IP-in-IP, and GRE operate at the network layer.

What are some other tunneling protocols?

In addition to GRE, IPsec, IP-in-IP, and SSH, other tunneling protocols include:

- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Tunneling Protocol (SSTP)
- Layer 2 Tunneling Protocol (L2TP)
- Virtual Extensible Local Area Network (VXLAN)