# Basic Knowledge of IP Routing

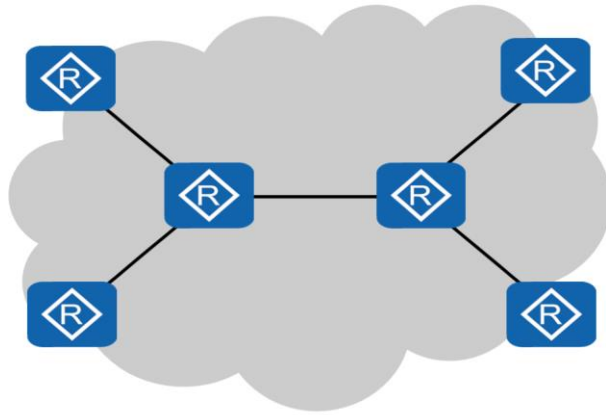
# Foreword

- The forwarding of frames and switching has introduced the data link layer operations, and in particular the role of IEEE 802 based standards as the supporting underlying communication mechanism, over which upper layer protocol suites generally operate. With the introduction of routing, the physics that define upper layer protocols and internetwork communication are established. An enterprise network domain generally consists of multiple networks for which routing decisions are needed to ensure optimal routes are used, in order to forward IP packets (or datagrams) to intended network destinations. This section introduces the foundations on which such IP routing is based.

# Objectives

- Upon completion of this section, you will be able to:
  - Explain the principles that govern IP routing decisions.
  - Explain the basic requirements for packet forwarding.

## Autonomous Systems



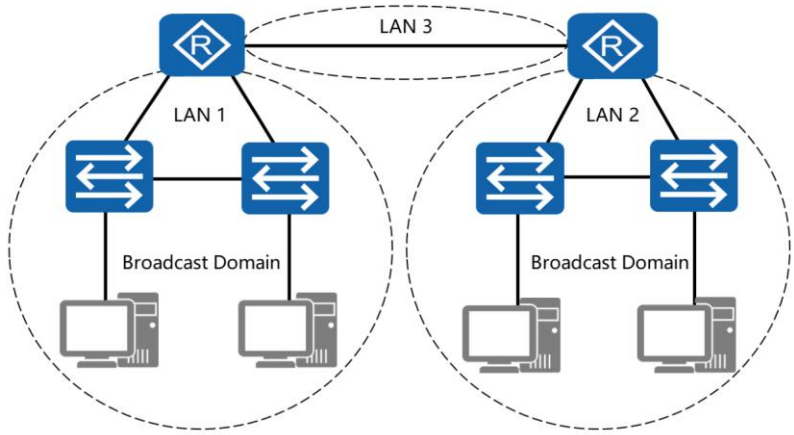
- An IP network, or networks, controlled by one or more operators with a clear policy that governs how routing decisions are made.





- An enterprise network generally can be understood as an instance of an autonomous system. As defined within RFC 1030, an autonomous system or AS, as it is also commonly known, is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy.
- The concept of autonomous systems originally considered the existence of a single routing protocol, however as networks have evolved, it is possible to support multiple routing protocols that interoperate through the injection of routes from one protocol to another. A routing policy can be understood to be a set of rules that determine how traffic is managed within an autonomous system, to which a single, or multiple operator(s) must adhere to.

# Local Area Network and Broadcast Domains

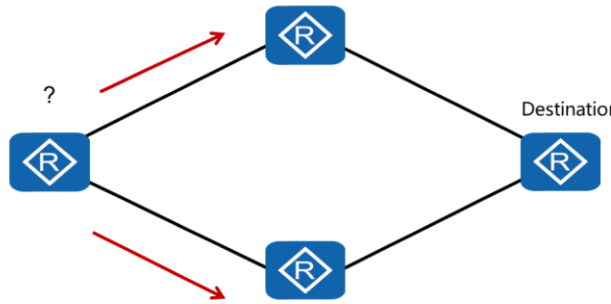







- The principles surrounding switching have dealt mainly with the forwarding of traffic within the scope of a local area network and the gateway, which has until now defined the boundary of the broadcast domain. Routers are the primary form of network layer device used to define the gateway of each local area network and enable IP network segmentation. Routers generally function as a means for routing packets from one local network to the next, relying on IP addressing to define the IP network to which packets are destined.

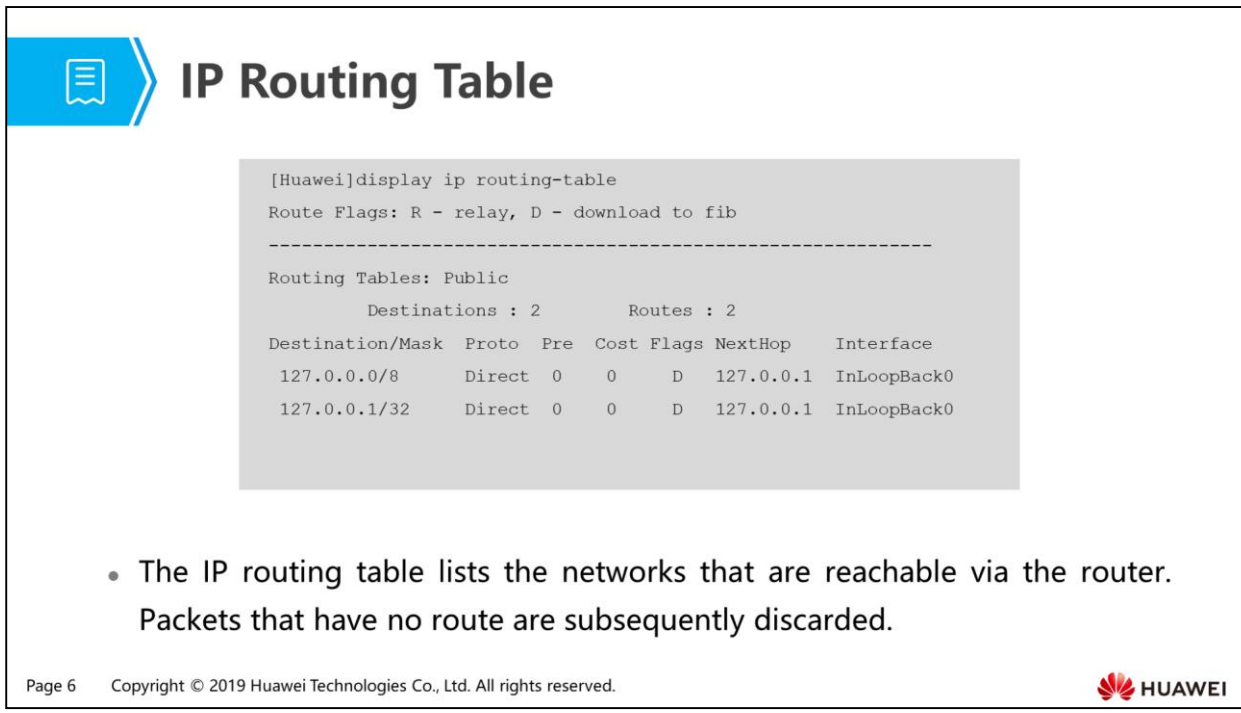
# Routing Decisions




- Routers are responsible for the decision making process that determines the path via which packets are forwarded.

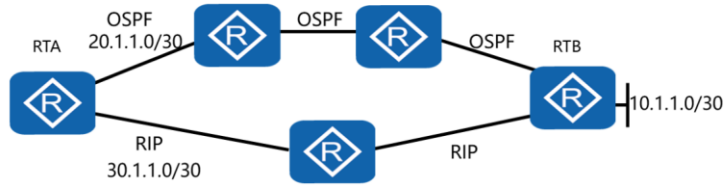
 

- The router is responsible for determining the forwarding path via which packets are to be sent the route to a given destination. It is the responsibility of each router to make decisions as to how the data is forwarded. Where a router has multiple paths to a given destination, route decisions based on calculations are made to determine the best next hop to the intended destination. The decisions governing the route that should be taken can vary depending on the routing protocol in use, ultimately relying on metrics of each protocol to make decisions in relation to varying factors such as bandwidth and hop count.




- Routers forward packets based on routing tables and a forwarding information base (FIB), and maintain at least one routing table and one FIB. Routers select routes based on routing tables and forward packets based on the FIB. A router uses a local routing table to store protocol routes and preferred routes. The router then sends the preferred routes to the FIB to guide packet forwarding. The router selects routes according to the priorities of protocols and costs stored in the routing table. A routing table contains key data for each IP packet.
- The destination & mask are used in combination to identify the destination IP address or the destination network segment where the destination host or router resides.
- The protocol (Proto) field, indicates the protocol through which routes are learned. The preference (Pre) specifies the preference value that is associated with the protocol, and is used to decide which protocol is applied to the routing table where two protocols offer similar routes. The router selects the route with the highest preference (the smallest value) as the optimal route.
- A cost value represents the metric that is used to distinguish when multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.
- A next-hop value indicates the IP address of the next network layer device or gateway that an IP packet passes through. In the example given a next-hop of 127.0.0.1 refers to the local interface of the device as being the next-hop.
- Finally the interface parameter indicates the outgoing interface through which an IP packet is forwarded.

# Routing Decisions – Preference




```
[RTA]display ip routing-table
Destination/Mask  Proto   Pre  Cost  Flags NextHop         Interface
10.1.1.0/30       OSPF    10   60    RD    20.1.1.2        Ethernet0/0/0
......
```

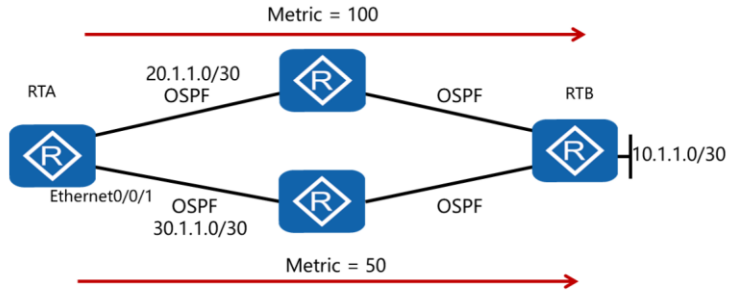
| Route | Direct | OSPF | Static | RIP |
|---|---|---|---|---|
| Preference | 0 | 10 | 60 | 100 |



HUAWEI

- A routing table may contain the routes originating from multiple protocols to a given destination. Not all routing protocols are considered equal, and where the longest match for multiple routes of differing routing protocols to the same destination are equal, a decision must be made regarding which routing protocol (including static routes) will take precedence.
- Only one routing protocol at any one time determines the optimal route to a destination. To select the optimal route, each routing protocol (including the static route) is configured with a preference (the smaller the value, the higher the preference). When multiple routing information sources coexist, the route with the highest preference is selected as the optimal route and added to the local routing table.
- In the example, two protocols are defined that provide a means of discovery of the 10.1.1.0 network via two different paths. The path defined by the RIP protocol appears to provide a more direct route to the intended destination, however due to the preference value, the route defined by the OSPF protocol is preferred and therefore installed in the routing table as the preferred route. A summary of the default preference values of some common routing mechanisms are provided to give an understanding of the default preference order.

# Routing Decisions – Metric



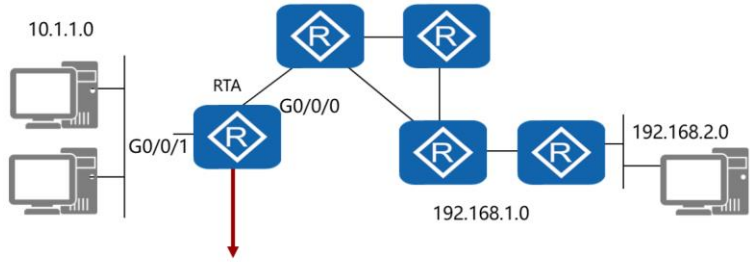

```
[RTA]display ip routing-table
Destination/Mask  Proto   Pre  Cost  Flags NextHop         Interface
10.1.1.0/30       OSPF    10   50    RD    30.1.1.2        Ethernet0/0/1
```





- Where the route is unable to be distinguished by either a longest match value or preference, the cost metric is taken as the decision maker in identifying the route that should be installed in the routing table. Cost represents the length of a path to a destination network.
- Each segment provides a cost metric value along a path that is combined to identify the cost of the route. Another common factor is network bandwidth, on which the cost mechanism is sometimes based. A link with a higher speed (capacity) represents a lower cost value, allowing preference of one path over another to be made, whilst links of equal speed are given a balanced cost for efficient load balancing purposes. A lower metric always takes precedence and therefore the metric of 50 as shown in the example, defines the optimal route to the given destination for which an entry can be found in the routing table.

# Establish IP Routing-table



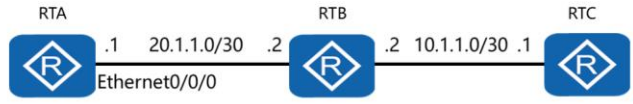

| 路由来源 | 目标网络 | 出接口 |
|---|---|---|
| Direct | 10.1.1.0 | G0/0/1 |
| Static | 192.168.1.0 | G0/0/0 |
| OSPF | 192.168.2.0 | G0/0/0 |





- By using the “preference” and the “cost”, IP Routing-table can be established.
- And the IP Routing-table can be devided into three kinds based on different source.
  - Direct routes
  - Static routes
  - Dynamic routes

## Routing Decisions – Longest Match



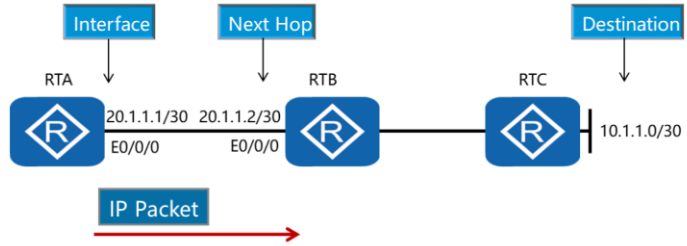

```
[RTA]display ip routing-table
Destination/Mask   Proto   Pre  Cost      Flags NextHop         Interface
10.1.1.0/24        Static  60   0           RD  20.1.1.2        Ethernet0/0/0
10.1.1.0/30        Static  60   0           RD  20.1.1.2        Ethernet0/0/0
```

- Routes to the same network destination will be initially compared and chosen based on a longest match.

- In order to allow packets to reach their intended destination, routers must make specific decisions regarding the routes that are learned and which of those routes are applied. A router is likely to learn about the path to a given network destination via routing information that is advertised from neighboring routers, alternatively it is possible for the statically applied routes to be manually implemented through administrator intervention.
- Each entry in the FIB table contains the physical or logical interface through which a packet is sent in order to reach the next router. An entry also indicates whether the packet can be sent directly to a destination host in a directly connected network. The router performs an "AND" operation on the destination address in the packet and the network mask of each entry in the FIB table.
- The router then compares the result of the "AND" operation with the entries in the FIB table to find a match. The router chooses the optimal route to forward packets according to the best or "longest" match. In the example, two entries to the network 10.1.1.0 exist with a next-hop of 20.1.1.2. Forwarding to the destination of 10.1.1.1 will result in the longest match principle being applied, for which the network address 10.1.1.0/30 provides the longest match.

# Routing Table Forwarding Requirements




- The forwarding of packets requires that the destination be known as well as the forwarding interface and next-hop.

- The capability of a router to forward an IP packet to a given destination requires that certain forwarding information be known. Any router wishing to forward an IP packet must firstly be aware of a valid destination address to which the packet is to be forwarded, this means that an entry must exist in the routing table that the router is able to consult. This entry must also identify the interface via which IP packets must be transmitted and the next-hop along the path, to which the packet is expected to be received before consultation for the next forwarding decision is performed.

# Summary

- What is the order in which routing decisions are made?
- What does the preference represent?

HUAWEI

- When router chooses the best route, first, put the routes with the smallest preference value into IP routing-table; if the priority is equal, then compares metric values to decide which routes to put into the routing table; finally, when looking up the routing table, it chooses the route items to guide the data packet forwarding according to the longest mask matching principle.
- The preference is typically used to denote the reliability of a route over routes that may be considered less reliable. Vendors of routing equipment may however assign different preference values for protocols that are supported within each vendors own product. The preference values of some common routing protocols supported by Huawei routing devices can be found within this section.


Thank You
www.huawei.com

# IP Static Routes

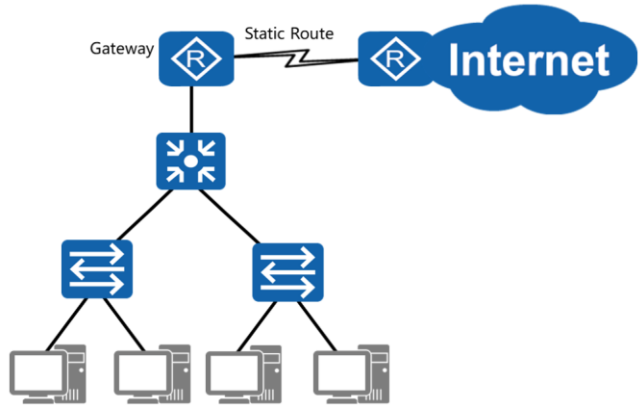
# Foreword

- The implementation of routes within the IP routing table of a router can be defined manually using static routes or through the use of dynamic routing protocols. The manual configuration of routes enables direct control over the routing table, however may result in route failure should a router' s next-hop fail. The configuration of static routes however is often used to compliment dynamic routing protocols to provide alternative routes in the event dynamically discovered routes fail to provide a valid next-hop. Knowledge of the various applications of static routes and configuration is necessary for effective network administration.

# Objectives

- Upon completion of this section, you will be able to:
  - Explain the different applications for static routes.
  - Successfully configure static routes in the IP routing table.

## Application for Static Route

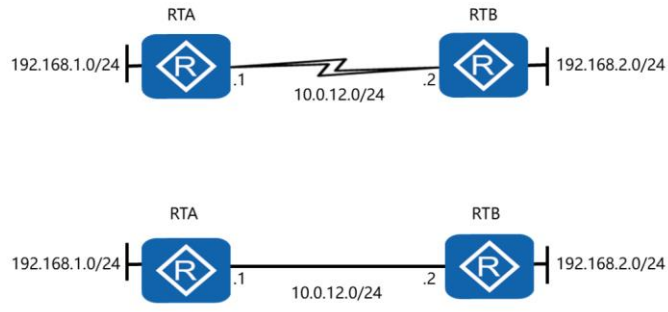



- Static routes define a means of path selection to other networks.

- A static route is a special route that is manually configured by a network administrator. The disadvantage of static routes is that they cannot adapt to the change in a network automatically, so network changes require manual reconfiguration. Static routes are fit for networks with comparatively simple structures. It is not advisable to configure and maintain static routes for a network with a complex structure. Static routes do however reduce the effect of bandwidth and CPU resource consumption that occurs when other protocols are implemented.

# Static Route Behavior



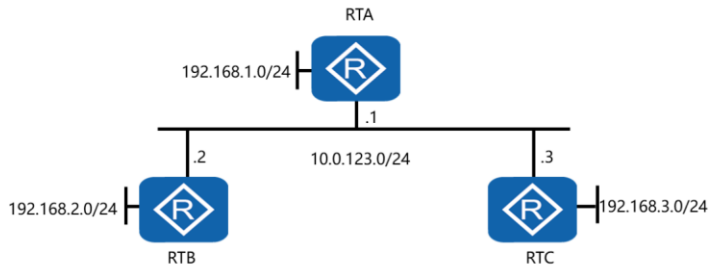

- The forwarding of packets based on a serial interface requires that the outbound interface be defined.



HUAWEI

- Static routes can be applied to networks that use both serial and Ethernet based media, however in each situation the conditions of applying the static route vary in which either the outbound interface or the next-hop IP address must be defined.
- The serial medium represents a form of point-to-point (P2P) interface for which the outbound interface must be configured. For a P2P interface, the next-hop address is specified after the outbound interface is specified. That is, the address of the remote interface (interface on the peer device) connected to this interface is the next-hop address.
- For example, the protocol used to encapsulate over the serial medium is the Point-to-Point protocol (PPP). The remote IP address is obtained following PPP negotiation, therefore it is necessary to specify only the outbound interface. The example also defines a form of point-to-point Ethernet connection, however Ethernet represents a broadcast technology in nature and therefore the principles of point-to-point technology do not apply.

# Static Route Behavior



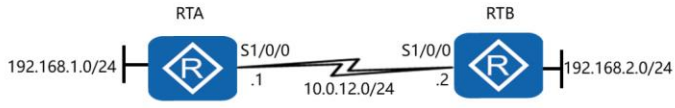

- The forwarding of packets over broadcast networks such as Ethernet, requires that the next-hop be defined.



HUAWEI

- In the case of broadcast interfaces such as Ethernet, the next-hop must be defined. Where the Ethernet interface is specified as the outbound interface, multiple next hops are likely to exist and the system will not be able to decide which next-hop is to be used. In determining the next-hop, a router is able to identify the local connection over which the packet should be received.
- In the example, packets intended for the destination of 192.168.2.0/24 should be forwarded to the next-hop of 10.0.123.2 to ensure delivery. Alternatively reaching the destination of 192.168.3.0 requires that the next-hop of 10.0.123.3 be defined.

# Configuring a Static Route




```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1
[RTB]ip route-static 192.168.1.0 255.255.255.0 Serial 1/0/0
[RTB]ip route-static 192.168.1.0 24 Serial 1/0/0
```

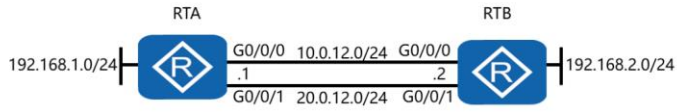
- A static route can be configured based on one of three variations.





- The configuration of the static route is achieved using the *ip route-static ip-address* { *mask* | *mask-length* } *interface-type interface-number* [ *nexthop-address* ] where the *ip-address* refers to the network or host destination address. The mask field can be defined as either a mask value or based on the prefix number. In the case of a broadcast medium such as Ethernet, the next-hop address is used. Where a serial medium is used, the interface-type and interface-number are assigned (e.g. serial 1/0/0) to the command to define the outgoing interface.

# Static Route Load Balancing




```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1
[RTB]ip route-static 192.168.1.0 255.255.255.0 20.0.12.1
```

- Static routes support load balancing to the same destination where the cost of routes are equal.



HUAWEI

- Where equal cost paths exist between the source and destination networks, load balancing can be implemented to allow traffic to be carried over both links. In order to achieve this using static routes, both routes must meet the parameters for an equal longest match, preference and metric value. The configuration of multiple static routes, one for each next-hop or outbound interface in the case of serial medium is required.
- The example demonstrates how two *ip route-static* commands are implemented, each defining the same IP destination address and mask, but alternate next-hop locations. This ensures that the longest match (/24) is equal, and naturally so is the preference value, since both routes are static routes that carry a default preference of 60. The cost of both paths is also equal allowing load balancing to occur.

# Verifying Static Route Load Balancing

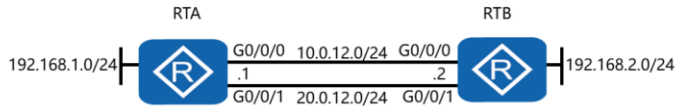
```
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public         Destinations : 13        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

......
192.168.1.0/24     Static  60   0           RD  10.0.12.1       GigabitEthernet 0/0/0
                   Static  60   0           RD  20.0.12.1       GigabitEthernet 0/0/1
```





- The routing table can be queried to verify the results by running the *display ip routing-table* command after the static routes are configured. The static route is displayed in the routing table, and results show two entries to the same destination, with matching preference and metric values. The different next-hop addresses and variation in the outbound interface identifies the two paths that are taken, and confirms that load balancing has been achieved.

# Floating Static Routes




```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1
[RTB]ip route-static 192.168.1.0 255.255.255.0 20.0.12.1
preference 100
```

- Floating static routes provide an alternative route in the event that the primary static route fails.



HUAWEI

- The application of static routes allows for a number of ways that routes can be manipulated to achieve routing requirements. It is possible for the preference of a static route to be changed for the purpose of enabling the preference of one static route over another, or where used with other protocols, to ensure the static route is either preferred or preference is given to the alternative routing protocol.
- The default preference value of a static route is 60, therefore by adjusting this preference value, a given static route can be treated with unequal preference over any other route, including other static routes. In the example given, two static routes exist over two physical LAN segments, while normally both static routes would be considered equal, the second route has been given a lesser preference (higher value) causing it to be removed from the routing table. The principle of a floating static route means that the route with a lesser preference will be applied to the routing table, should the primary route ever fail.

## Floating Static Route Check

```
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public         Destinations : 13        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

......
192.168.1.0/24  Static  60   0           RD  10.0.12.1       GigabitEthernet0/0/0
```

- Prior to the failure of the primary route, only the primary static route will be present within the routing table.

- In using the *display ip routing-table* command, it is possible for the results of the change to the preference value that results in the floating static route, to be observed. Normally two equal cost routes would be displayed in the routing table defining the same destination, however having alternative next-hop values and outbound interfaces. In this case however, only one instance can be seen, containing the default static route preference value of 60. Since the second static route now has a preference value of 100, it is not immediately included in the routing table since it is no longer considered an optimal route.

## Floating Static Route Check

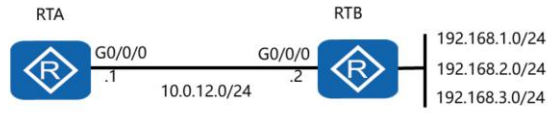
```
[RTB]interface GigabitEthernet 0/0/0
[RTB-GigabitEthernet 0/0/0]shutdown
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public         Destinations : 13        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
......
192.168.1.0/24 Static  100  0  RD  20.0.12.1 GigabitEthernet 0/0/1
```

- In disabling the primary route, the floating static route is then added to the routing table.

- In the event that the primary static route should fail as a result of physical link failure or through the disabling of an interface, the static route will no longer be able to provide a route to the intended destination and therefore will be removed from the routing table. The floating static route is likely to become the next best option for reaching the intended destination, and will be added to the routing table to allow packets to be transmitted over a second alternative path to the intended destination, allowing continuity in light of any failure.
- When the physical connection for the original route is restored, the original static route also will take over from the current floating static route, for which the route will be restored in the routing table causing the floating static route to once again await application.

# Default Static Routes




```
[RTA]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
```

- Default routes provide a form of last resort route in the event that no other longest match is found within the routing table.

- The default static route is a special form of static route that is applied to networks in which the destination address is unknown, in order to allow a forwarding path to be made available. This provides an effective means of routing traffic for an unknown destination to a router or gateway that may have knowledge of the forwarding path within an enterprise network.
- The default route relies on the "any network" address of 0.0.0.0 to match any network to which a match could not be found in the routing table, and provides a default forwarding path to which packets for all unknown network destinations should be routed. In the example, a default static route has been implemented on RTA, identifying that should packets for a network that is unknown be received, such packets should be forwarded to the destination 10.0.12.2.
- In terms of routing table decision making, as a static route, the default route maintains a preference of 60 by default, however operates as a last resort in terms of the longest match rule in the route matching process.

# Default Static Route Check

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public         Destinations : 13        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
.....
 0.0.0.0/0      Static  60   0  RD   10.0.12.2 GigabitEthernet0/0/0
```

- The configuration of the static route once configured will appear within the routing table of the router. The *display ip routing-table* command is used to view this detail. As a result, all routes in the example where not associated with any other routes in the routing table will be forwarded to the next-hop destination of 10.0.12.2 via the interface Gigabit Ethernet 0/0/0.

# Summary

- What should be altered to enable a static route to become a floating static route?
- Which network address should be defined to allow a default static route to be implemented in the routing table?

HUAWEI

- A floating static route can be implemented by adjusting the preference value of a static route where two static routes support load balancing.
- A default static route can be implemented in the routing table by specifying the 'any network' address of 0.0.0.0 as the destination address along with a next-hop address of the interface to which packets captured by this default static route are to be forwarded.


Thank You
www.huawei.com

# Link State Routing with OSPF

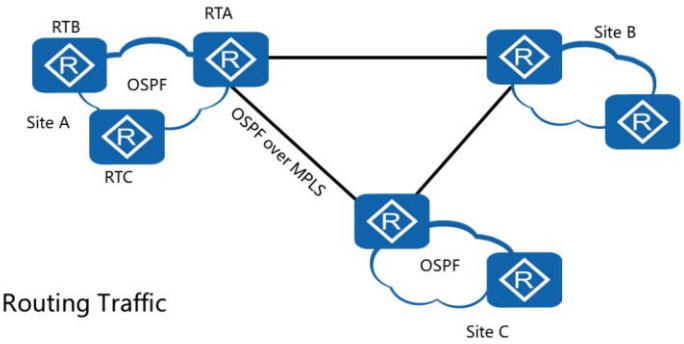
# Foreword

- OSPF is an interior gateway protocol (IGP) designed for IP networks, that is founded on the principles of link state routing. The link state behavior provides many alternative advantages for medium and even large enterprise networks. Its application as an IGP is introduced along with information relevant to the understanding of OSPF convergence and implementation, for supporting OSPF in enterprise networks.

# Objectives

- Upon completion of this section, you will be able to:
  - Explain the OSPF convergence process.
  - Describe the different network types supported by OSPF.
  - Successfully configure single area OSPF networks.

# Open Shortest Path First (OSPF)



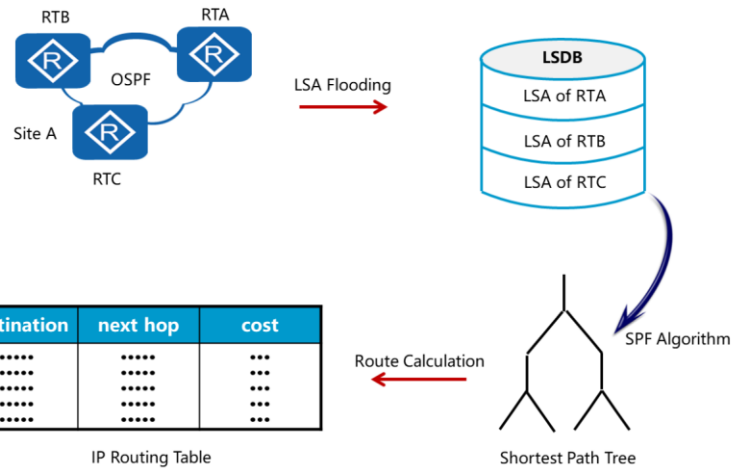

- Minimal Routing Traffic
- Rapid Convergence
- Scalable
- Accurate Route Metrics





- Open Shortest Path First or OSPF is regarded as a link state protocol that is capable of quickly detecting topological changes within the autonomous system and establish loop free routes in a short period of time, with minimum additional communication overhead for negotiating topology changes between peering routers. OSPF also deals with scalability issues that occur when communication between an expanding number of routers becomes so extreme that it begins to lead to instability within the autonomous system. This is managed through the use of areas that limits the scope of router communication to an isolated group within the autonomous system allowing small, medium and even large networks to be supported by OSPF. The protocol is also able to work over other protocols such as MPLS, a label switching protocol, to provide network scalability even over geographically disperse locations. In terms of optimal path discovery, OSPF provides rich route metrics that provides more accuracy than route metrics applied to protocols such as RIP to ensure that routes are optimized, based on not only distance but also link speed.

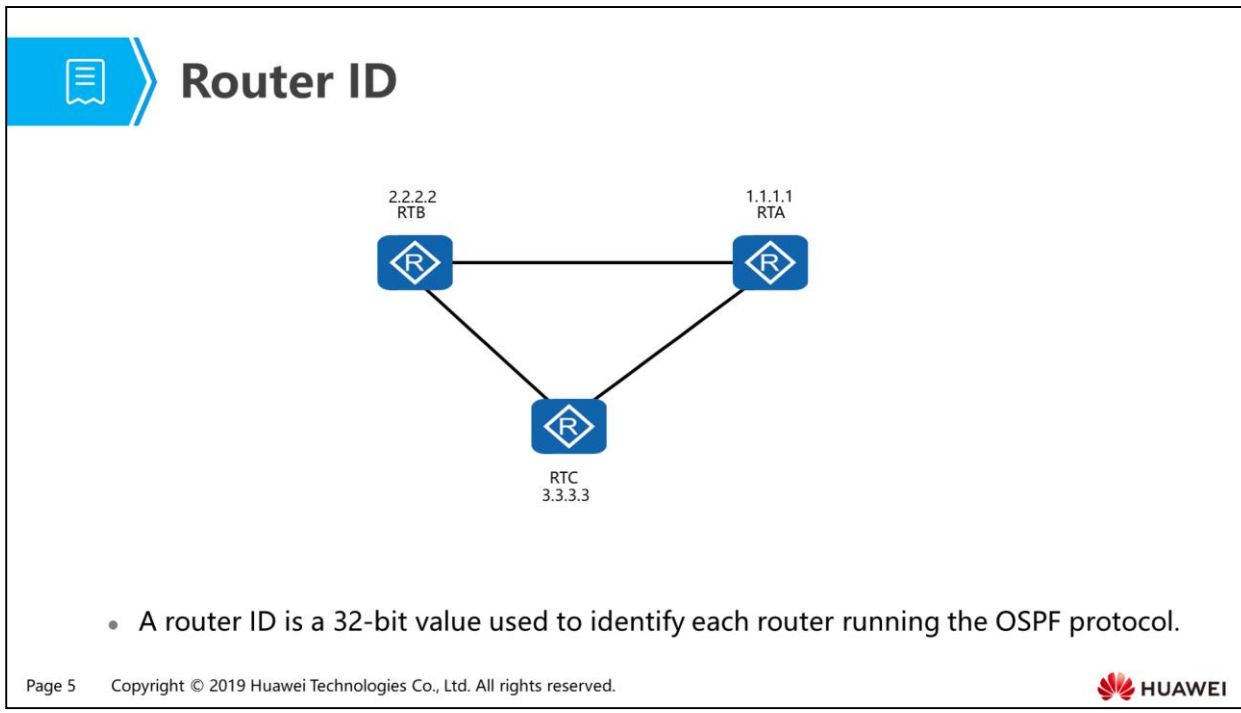
# OSPF Convergence Behavior





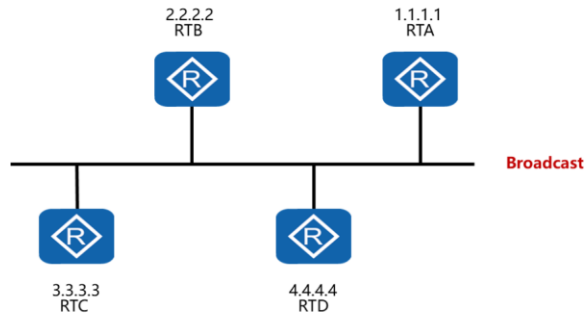

HUAWEI

- The convergence of OSPF requires that each and every router actively running the OSPF protocol have knowledge of the state of all interfaces and adjacencies (relationship between the routers that they are connected to), in order to establish the best path to every network. This is initially formed through the flooding of Link State Advertisements (LSA) which are units of data that contain information such as known networks and link states for each interface within a routing domain. Each router will use the LSA received to build a link state database (LSDB) that provides the foundation for establishing the shortest path tree to each network, the routes from which are ultimately incorporated into the IP routing table.




- The router ID is a 32-bit value assigned to each router running the OSPF protocol. This value uniquely identifies the router within an Autonomous System. The router ID can be assigned manually, or it can be taken from a configured address. If a logical (loopback) interface has been configured, the router ID will be based upon the IP address of the highest configured logical interface, should multiple logical interfaces exist.
- If no logical interfaces have been configured, the router will use the highest IP address configured on a physical interface. Any router running OSPF can be restarted using the graceful restart feature to renew the router ID should a new router ID be configured. It is recommended that the router ID be configured manually to avoid unexpected changes to the router ID in the event of interface address changes.

# OSPF Supported Network Types



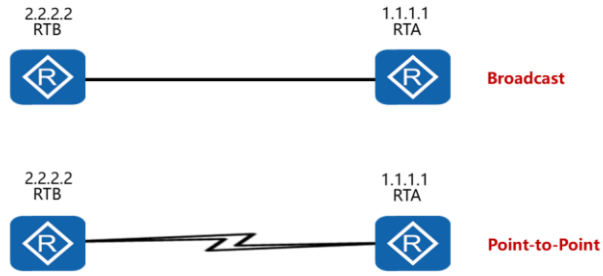

- Ethernet based networks adopt the broadcast network type by default.





- OSPF supports various network types, and in each case will apply a different behavior in terms of how neighbor relationships are formed and how communication is facilitated. Ethernet represents a form of broadcast network that involves multiple routers connected to the same network segment. One of the primary issues faced regards how communication occurs between the neighboring routers in order to minimize OSPF routing overhead. If an Ethernet network is established, the broadcast network type will be applied automatically in OSPF.

# OSPF Supported Network Types



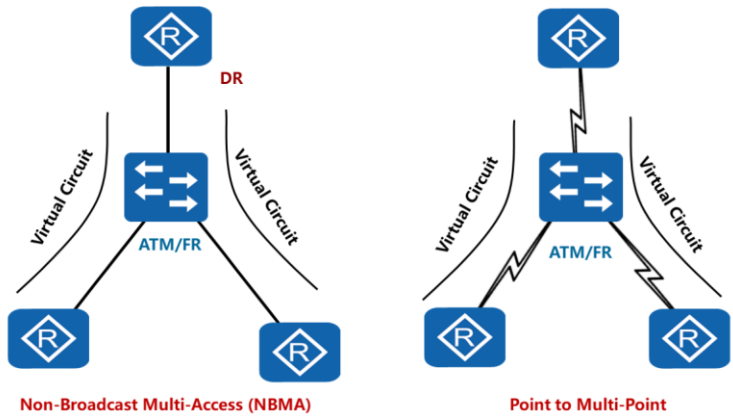

- Serial technologies such as PPP and HDLC will default to the Point-to-Point network type.





- Where two routers are established in a point-to-point topology, the applied network type will vary depending on the medium and link layer technology applied. As mentioned, the use of an Ethernet medium will result in the broadcast network type for OSPF being assigned automatically. Where the physical medium is serial, the network type is considered point-to-point. Common forms of protocols that operate over serial media at the link layer include Point-to-Point Protocol (PPP) and High-level Data Link Control (HDLC).

# OSPF Supported Network Types



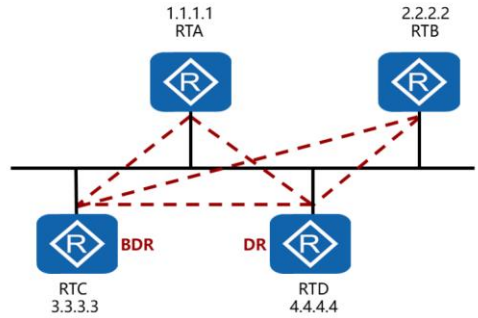

- ATM & Frame Relay default to Non-Broadcast Multi-Access.





- OSPF may operate over multi access networks that do not support broadcasts. Such networks include Frame Relay and ATM that commonly operate using hub and spoke type topologies, which rely on the use of virtual circuits in order for communication be to achieved. OSPF may specify two types of networks that can be applied to links connected to such environments. The Non-Broadcast Multi Access (NBMA) network type emulates a broadcast network and therefore requires each peering interface be part of the same network segment. Unlike a broadcast network, the NBMA forwards OSPF packets as a unicast, thereby requiring multiple instances of the same packet be generated for each destination.
- Point-to-Multipoint may also be applied as the network type for each interface, in which case a point-to-point type behavior is applied. This means that each peering must be associated with different network segments. Designated Routers are associated with broadcast networks, and therefore are implemented by NBMA networks. Most importantly is the positioning of a DR which must be assigned on the hub node of the hub and spoke architecture to ensure all nodes can communicate with the DR.

## Designated Router & Backup Designated Router



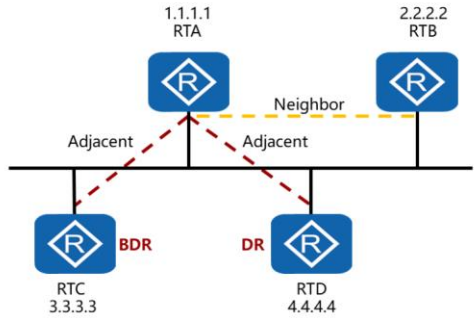

- Designated Routers limit the number of adjacencies necessary in broadcast (Ethernet) networks.



HUAWEI

- In order to address and optimize the communication of OSPF over broadcast networks, OSPF implements a Designated Router (DR) that acts as a central point of communication for all other routers associated with a broadcast network on at least one interface. In a theoretical broadcast network that does not apply a DR, it can be understood that the communication follows an n(n-1)/2 formula, where n represents the number of router interfaces participating in OSPF. In the example given, this would refer to 6 adjacencies between all routers. When the DR is applied, all routers establish a relationship with the DR to which is responsible for acting as a central point of communication for all neighboring routers in a broadcast network.
- A Backup Designated Router (BDR) is a router that is elected to take over from the DR should it fail. As such it is necessary that the BDR establish a link state database as that of the DR to ensure synchronization. This means that all neighboring routers must also communicate with the BDR in a broadcast network. With the application of the DR and BDR, the number of associations is reduced from 6 to 5 since RTA and RTB need only communicate with the DR and BDR. This may appear to have a minimal effect however where this is applied to a network containing for example 10 routers, i.e. (10*9)/2 the resulting communication efficiency becomes apparent.

# Neighbor States



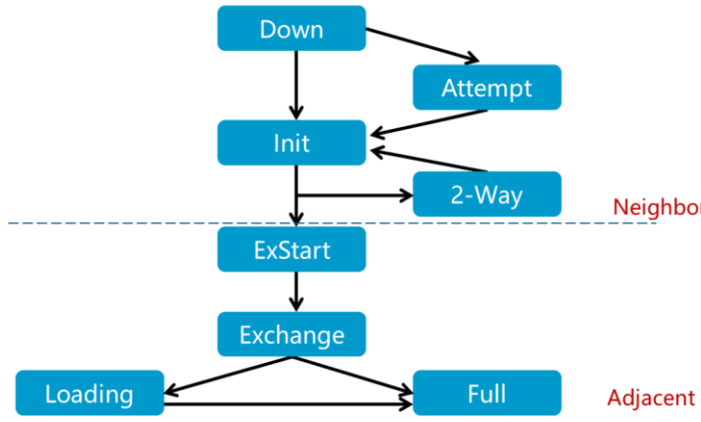

- Defines form of relationship between neighbors.
- Two neighbor states are possible, neighbor and adjacent.

HUAWEI

- OSPF creates adjacencies between neighboring routers for the purpose of exchanging routing information. Not every two neighboring routers will become adjacent, particularly where one of the two routers establishing an adjacency is considered to not be the DR or BDR. These routers are known as DROther and only acknowledge the presence of the DROther but do not establish full communication; this state is known as the neighbor state. DROther routers do however form full adjacency with both DR and BDR routers to allow synchronization of the link state database of the DR and BDR routers with each of the DROther routers. This synchronization is achieved by establishing an adjacent state with each DROther.
- An adjacency is bound to the network that the two routers have in common. If two routers have multiple networks in common, they may have multiple adjacencies between them.

## Link State Establishment

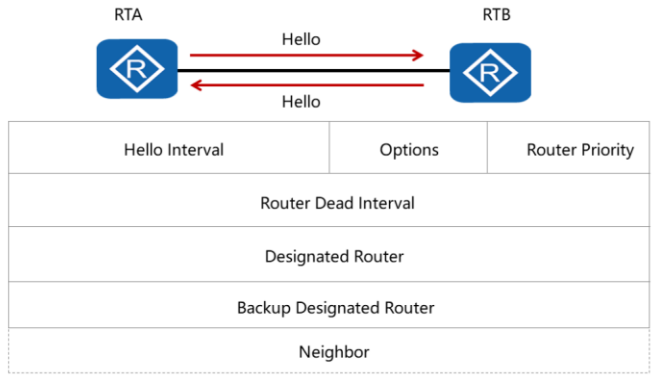



- State changes allow for neighbor relationships to be achieved.

- Each router participating in OSPF will transition through a number of link states to achieve either a neighbor state or an adjacent state. All routers begin in the down state upon initialization and go through a neighbor discovery process, which involves firstly making a routers presence known within the OSPF network via a Hello packet. In performing this action the router will transition to an init state.
- Once the router receives a response in the form of a Hello packet containing the router ID of the router receiving the response, a 2-way state will be achieved and a neighbor relationship formed. In the case of NBMA networks, an attempt state is achieved when communication with the neighbor has become inactive and an attempt is being made to re-establish communication through periodic sending of Hello packets. Routers that do not achieve an adjacent relationship will remain in a neighbor state with a 2-way state of communication.
- Routers such as DR and BDR will build an adjacent neighbor state with all other neighboring routers, and therefore must exchange link state information in order to establish a complete link state database. This requires that peering routers that establish an adjacency first negotiate for exchange of link state information (ExStart) before proceeding to exchange summary information regarding the networks they are aware of. Neighbors may identify routes they are either not aware of or do not have up to date information for, and therefore request additional details for these routes as part of the loading state. A fully synchronized relationship between neighbors is determined by the full state at which time both peering routers can be considered adjacent.

# Neighbor Discovery

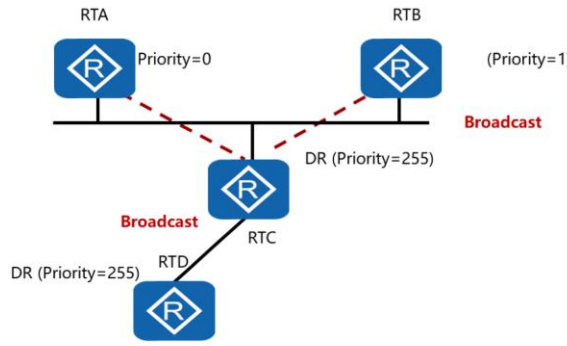



- The Hello protocol is responsible for neighbor discovery and maintenance for two way communication between neighbors.

- Neighbor discovery is achieved through the use of Hello packets that are generated at intervals based on a Hello timer, which by default is every 10 seconds for broadcast and point-to-point network types; whereas for NBMA and Point-to-Multipoint network types the hello interval is 30 seconds. The hello packet contains this interval period, along with a router priority field that allows neighbors to determine the neighbor with the highest router ID for identification of the DR and BDR in broadcast and NBMA networks.
- A period specifying how long a hello packet is valid before the neighbor is considered lost must also be defined, and this is carried as the router dead interval within the hello packet. This dead interval is set by default to be four times the hello interval, thus being 40 seconds for broadcast and point-to-point networks, and 120 seconds for NBMA and Point-to-Multipoint networks. Additionally, the router ID of both the DR and BDR are carried, where applicable, based on the network for which the hello packet is generated.

# Designated Router Election




```
[RTD]interface GigabitEthernet0/0/0
[RTD-GigabitEthernet0/0/0]ospf network-type p2p
```

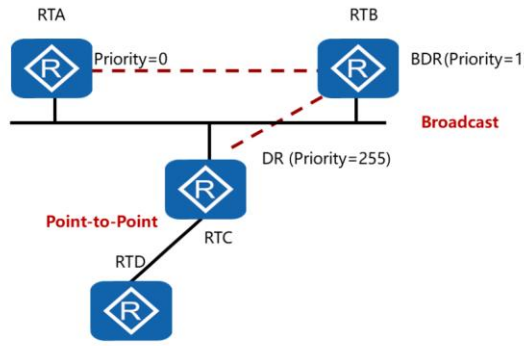
- A Designated Router is elected based on the priority value.

HUAWEI

- Following neighbor discovery, the DR election may occur depending on the network type of the network segment. Broadcast and NMBA networks will perform DR election. The election of the DR relies on a priority that is assigned for each interface that participates in the DR election process. This priority value is set as 1 by default and a higher priority represents a better DR candidate.
- If a priority of 0 is set, the router interface will no longer participate in the election to become the DR or BDR. It may be that where point-to-point connections (using Ethernet as the physical medium) are set to support a broadcast network type, unnecessary DR election will occur, which generates excessive protocol traffic. It therefore is recommended that the network type be configured as a point-to-point network type.

# Backup Designated Router Election

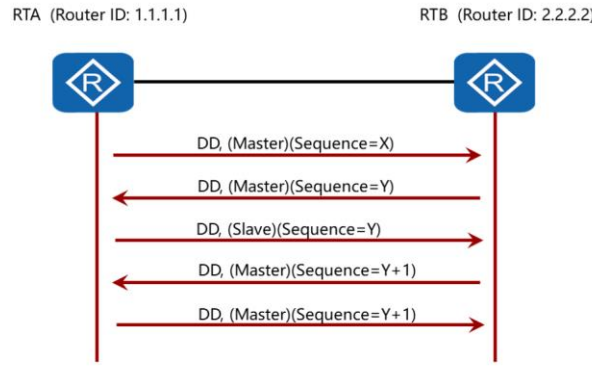



- The Backup Designated Router (BDR) forms adjacencies with all other routers and will become the DR if the existing DR fails.

- In order to make improve the efficiency of transition to a new Designated Router, a Backup Designated Router is assigned for each broadcast and NBMA network. The Backup Designated Router is also adjacent to all routers on the network, and becomes the Designated Router when the previous Designated Router fails. If there were no Backup Designated Router present, new adjacencies would have to be formed between the new Designated Router and all other routers attached to the network.
- Part of the adjacency forming process involves the synchronizing of link-state databases, which can potentially take quite a long time. During this time, the network would not be available for the transit of data. The Backup Designated Router obviates the need to form these adjacencies, since they already exist. This means the period of disruption in transit traffic lasts only as long as it takes to flood the new LSAs (which announce the new Designated Router). The Backup Designated Router is also elected by the Hello packet. Each Hello packet has a field that specifies the Backup Designated Router for the network.

# Database Synchronization



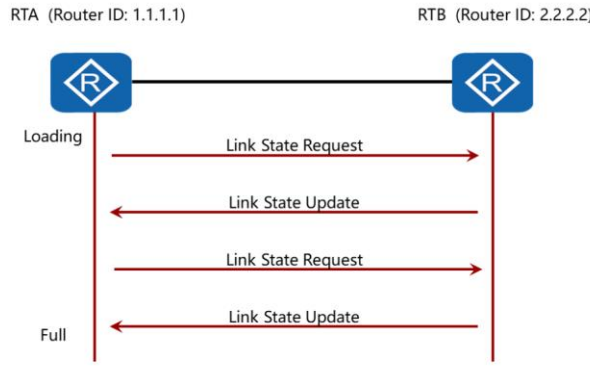

- Neighboring routers form a master/slave relationship.
- Database Description packets contain LSA header information.

HUAWEI

- In a link-state routing algorithm, it is very important for all routers' link-state databases to stay synchronized. OSPF simplifies this by requiring only adjacent routers remain synchronized. The synchronization process begins as soon as the routers attempt to bring up the adjacency. Each router describes its database by sending a sequence of Database Description packets to its neighbor. Each Database Description packet describes a set of LSAs belonging to the router's database.
- When the neighbor sees an LSA that is more recent than its own database copy, it makes a note that this newer LSA should be requested. This sending and receiving of Database Description packets is called the "Database Exchange Process". During this process, the two routers form a master/slave relationship. Each Database Description packet has a sequence number. Database Description packets sent by the master are acknowledged by the slave through echoing of the sequence number.

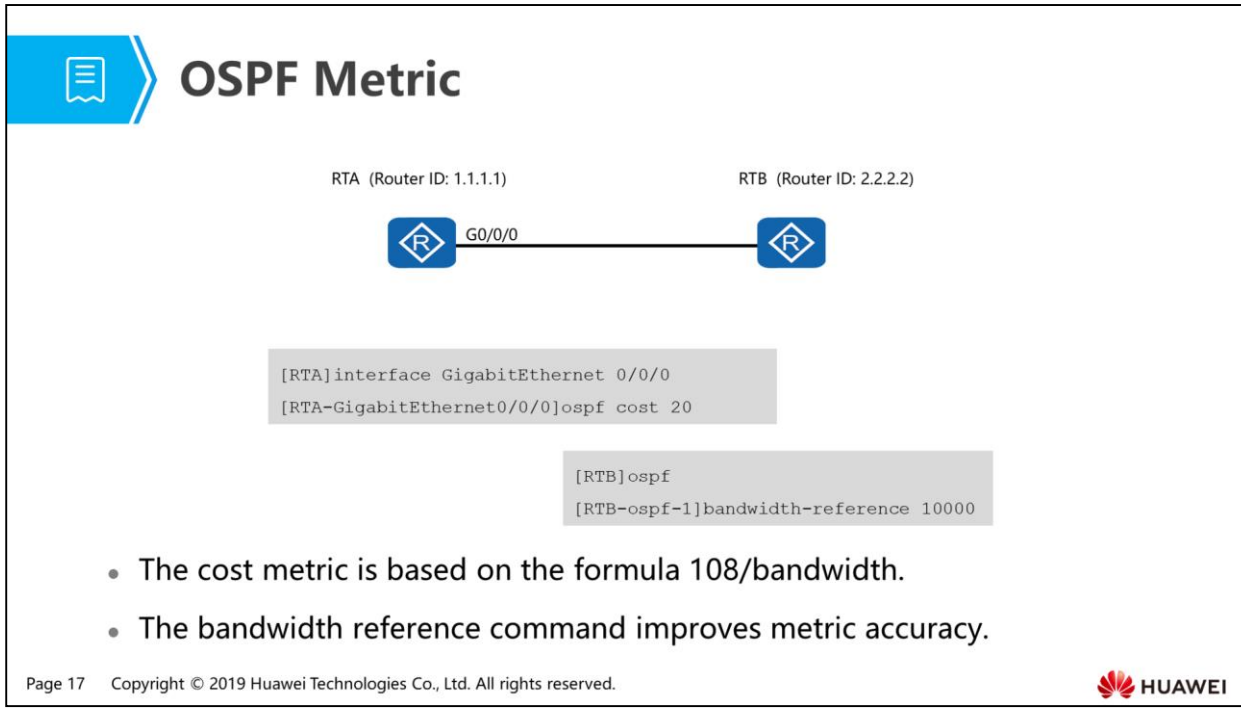
# Establishing Full Adjacency




- Missing or newer instances of LSA are requested using LSR.
- The entire requested LSA is sent as an update.

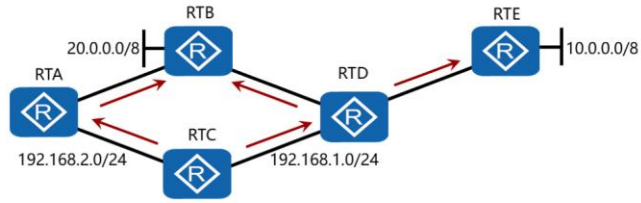
 

- During and after the Database Exchange Process, each router has a list of those LSAs for which the neighbor has more up-to-date instances. The Link State Request packet is used to request the pieces of the neighbor's database that are more up-to-date. Multiple Link State Request packets may need to be used.
- Link State Update packets implement the flooding of LSAs. Each Link State Update packet carries a collection of LSAs one hop further from their origin. Several LSAs may be included in a single packet. On broadcast networks, the Link State Update packets are multicast. The destination IP address specified for the Link State Update Packet depends on the state of the interface. If the interface state is DR or Backup, the address AllSPFRouters (224.0.0.5) should be used. Otherwise, the address AllDRouters (224.0.0.6) should be used. On non-broadcast networks, separate Link State Update packets must be sent, as unicast, to each adjacent neighbor (i.e. those in a state of Exchange or greater). The destination IP addresses for these packets are the neighbors' IP addresses.
- When the Database Description Process has completed and all Link State Requests have been satisfied, the databases are deemed synchronized and the routers are marked fully adjacent. At this time the adjacency is fully functional and is advertised in the two routers' router-LSAs.




- OSPF calculates the cost of an interface based on bandwidth of the interface. The calculation formula is: cost of the interface=reference value of bandwidth/bandwidth. The reference value of bandwidth is configurable for which the default is 100 Mbps. With the formula 100000000/Bandwidth, this gives a cost metric of 1562 for a 64 kbit/s Serial port, 48 for an E1 (2.048 Mbit/s) interface and a cost of 1 for Ethernet (100 Mbit/s) or higher.
- To be able to distinguish between higher speed interfaces it is imperative that the cost metric be adjusted to match the speeds currently supported. The bandwidth-reference commands allows the metric to be altered by changing the reference value of the bandwidth in the cost formula. The higher the value, the more accurate the metric. Where speeds of 10Gb are being supported, it is recommended that the bandwidth-reference value be increased to ‘10000’ or 1010/bandwidth to provide metrics of 1, 10 and 100 for 10Gb, 1Gb and 100Mb bandwidth links respectively.
- Alternatively the cost can be manually configured by using the ospf cost command to define a cost value for a given interface. The cost value ranges from 1 to 65535 with a default cost value of 1.

# Shortest Path Tree




```
[RTC]display ip routing-table
......
Destination/Mask  Proto  Pre  Cost      Flags NextHop         Interface
 10.0.0.0/8       OSPF   10   20          D   192.168.1.4     G0/0/0
 20.0.0.0/8       OSPF   10   20          D   192.168.1.4     G0/0/0
                  OSPF   10   20          D   192.168.2.1     G0/0/1
```

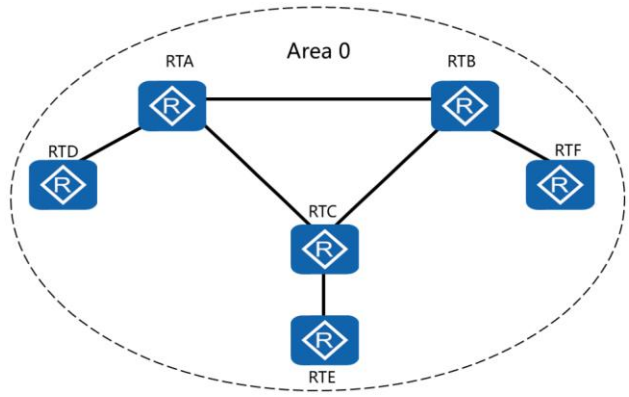
- Each router calculates the shortest path to all other networks.

HUAWEI

- A router that has achieved a full state is considered to have received all link state advertisements (LSA) and synchronized its link state database (LSDB) with that of the adjacent neighbors. The link state information collected in the link state database is then used to calculate the shortest path to each network. Each router only relies on the information in the LSDB in order to independently calculate the shortest path to each destination, as opposed to relying on select route information from peers which is deemed to be the best route to a destination. The calculation of the shortest path tree however means that each router must utilize additional resources to achieve this operation.

# OSPF Areas – Single Area



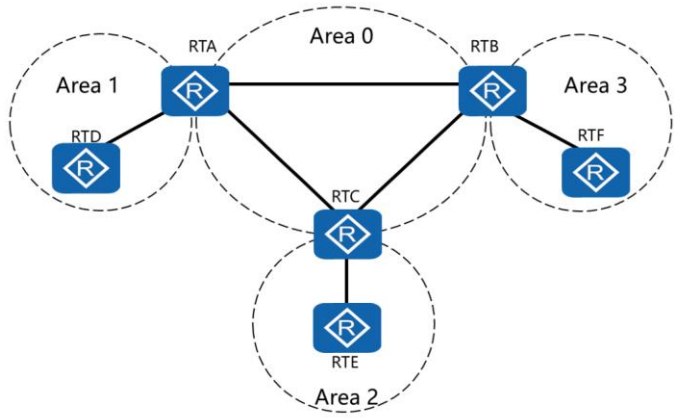

- A single link state database for the administrative domain.
- Any area number can be assigned but area 0 is recommended.

HUAWEI

- Smaller networks may involve a select number of routers which operate as part of the OSPF domain. These routers are considered to be part of an area which is represented by an identical link state database for all routers within the domain. As a single area, OSPF can be assigned any area number, however for the sake of future design implementation it is recommended that this area be assigned as area 0.

# OSPF Areas – Multi Area

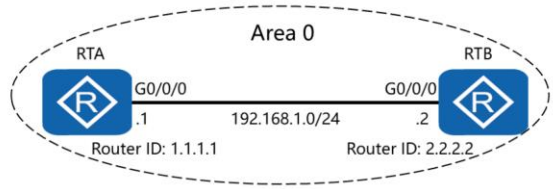



- Areas build separate LS databases, minimize impact of change.

- The need to forward link state advertisements and subsequent calculation of the shortest path based on the link state database becomes increasingly complex as more and more routers become a part of the OSPF domain. As such, OSPF is capable of supporting a hierarchical structure to limit the size of the link state database, and the number of calculations that must be performed when determining the shortest path to a given network.
- The implementation of multiple areas allows an OSPF domain to compartmentalize the calculation process based on a link state database that is only identical for each area, but provides the information to reach all destinations within the OSPF domain. Certain routers known as area border routers (ABR) operate between areas and contain multiple link state databases for each area that the ABR is connected to. Area 0 must be configured where multi-area OSPF exists, and for which all traffic sent between areas is generally required to traverse area 0, in order to ensure routing loops do not occur.

# OSPF Network Advertisement




```
[RTA]ospf 1 router-id 1.1.1.1
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
```

- The network command defines the network to be advertised.
- Route advertisements are forwarded based on areas.

  HUAWEI

- Establishing of OSPF within an AS domain requires that each router that is to participate in OSPF first enable the OSPF process. This is achieved using the ospf [process id] command, where the process ID can be assigned and represents the process with which the router is associated. If routers are assigned different process ID numbers, separate link state databases will be created based on each individual process ID. Where no process ID is assigned, the default process ID of 1 will be used. The router ID can also be assigned using the command ospf [process id] [router-id <router-id>], where <router-id> refers to the ID that is to be assigned to the router, bearing in mind that a higher ID value represents the DR in broadcast and NBMA networks.
- The parenthesis information reflects the ospf process and level at which ospf parameters can be configured, including the area to which each link (or interface) is associated. Networks that are to be advertised into a given area are determined through the use of the network command. The mask is represented as a wildcard mask for which a bit value of 0 represents the bits that are fixed (e.g. network id) and where the bit values in the mask represent a value of 1, the address can represent any value.

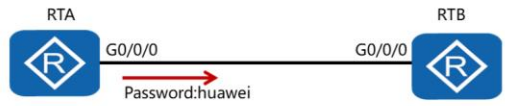
# Configuration Validation

```
[RTA]display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
                 Neighbors

Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet0/0/0)'s neighbors
Router ID: 2.2.2.2          Address: 192.168.1.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.2  BDR: 192.168.1.1  MTU: 0
   Dead timer due in 40  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:31
   Authentication Sequence: [ 0 ]
```

- Configuration of the neighbor relationship between OSPF peers is verified through the display ospf peer command. The attributes associated with the peer connection are listed to provide a clear explanation of the configuration. Important attributes include the area in which the peer association is established, the state of the peer establishment, the master/slave association for adjacency negotiation in order to reach the full state, and also the DR and BDR assignments which highlights that the link is associated with a broadcast network type.

# OSPF Authentication




```
[RTA]interface GigabitEthernet0/0/0
[RTA-GigabitEthernet0/0/0]ospf authentication-mode md5 1 huawei
```

- OSPF supports two forms of authentication, simple password or cryptographic authentication.

  HUAWEI

- OSPF is capable of supporting authentication to ensure that routes are protected from malicious actions that may result from manipulation or damage to the existing OSPF topology and routes. OSPF allows for the use of simple authentication as well as cryptographic authentication, which provides enhanced protection against potential attacks.
- Authentication is assigned on a per interface basis with the command for simple authentication of ospf authentication-mode { simple [ [ plain ] <plain-text> | cipher <cipher-text >] | null } where plain applies a clear-text password, cipher a cipher-text password to hide the original contents, and null to indicate a null authentication.
- Cryptographic authentication is applied using the ospf authentication-mode { md5 | hmac-md5 } [ key-id { plain <plain-text >| [ cipher ] <cipher-text >} ] command. MD5 represents a cryptographic algorithm for securing authentication over the link, with its configuration demonstrated within the given example. The key identifies a unique authentication key ID of the cipher authentication of the interface. The key ID must be consistent with that of the peer.

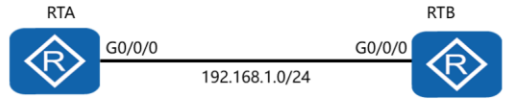
# Configuration Validation

```
<RTA>terminal debugging
<RTA>debugging ospf packet
Aug 19 2013 08:10:06.850.2+00:00 RTA RM/6/RMDEBUG:  Source Address:
192.168.1.1
Aug 19 2013 08:10:06.850.3+00:00 RTA RM/6/RMDEBUG:  Destination
Address: 224.0.0.5
……
Aug 19 2013 08:10:06.850.6+00:00 RTA RM/6/RMDEBUG:  Area: 0.0.0.0,
Chksum: 0
Aug 19 2013 08:10:06.850.7+00:00 RTA RM/6/RMDEBUG:  AuType: 02
Aug 19 2013 08:10:06.850.8+00:00 RTA RM/6/RMDEBUG:  Key(ascii): * *
* * * * * *
```

- Where authentication is applied, it is possible to implement debugging on the terminal to view the authentication process. Since the debugging may involve many events, the debugging ospf packet command should be used to specify that debugging should only be performed for OSPF specific packets. As a result the authentication process can be viewed to validate that the authentication configuration has been successfully implemented.

# OSPF Silent Interface




```
[RTA]ospf
[RTA-ospf-1]silent-interface GigabitEthernet0/0/0
```

- The silent-interface command prevents an interface from forming neighbor relationships with peers.

  HUAWEI

- It is often necessary to control the flow of routing information and limit the range for which such routing protocols can extend. This is particularly the case where connecting with external networks from whom knowledge of internal routes is to be protected. In order to achieve this, the silent interface command can be applied as a means to restrict all OSPF communication via the interface on which the command is implemented.
- After an OSPF interface is set to be in the silent state, the interface can still advertise its direct routes. Hello packets on the interface, however, will be blocked and no neighbor relationship can be established on the interface. The command silent-interface [interface-type interface-number] can be used to define a specific interface that is to restrict OSPF operation, or alternatively the command silent-interface all can be used to ensure that all interfaces under a specific process be restricted from participating in OSPF.

# Configuration Validation

```
[RTA]display ospf 1 interface GigabitEthernet0/0/0

        OSPF Process 1 with Router ID 1.1.1.1
                Interfaces

 Interface: 192.168.1.1 (GigabitEthernet0/0/0)
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 192.168.1.1
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit
Delay 1
 Silent interface, No hellos
```

- The implementation of the silent interface on a per interface basis means that the specific interface should be observed to validate the successful application of the silent interface command. Through the display ospf <process_id> interface <interface> command, where the interface represents the interface to which the silent interface command has been applied, it is possible to validate the implementation of the silent interface.

# Summary

- What is the purpose of the dead interval in the OSPF header?
- In a broadcast network, what is the multicast address that is used by the Designated Router (DR) and Backup Designated Router (BDR) for listening for link state update information?

HUAWEI

- The dead interval is a timer value that is used to determine whether the propagation of OSPF Hello packets has ceased. This value is equivalent to four times the Hello interval, or 40 seconds by default on broadcast networks. In the event that the dead interval counts down to zero, the OSPF neighbor relationship will terminate.
- The DR and BDR use the multicast address 224.0.0.6 to listen for link state updates when the OSPF network type is defined as broadcast.


Thank You
www.huawei.com

# DHCP Protocol Principles

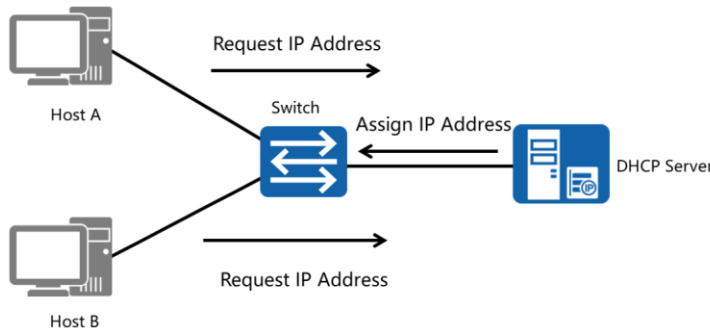
# Foreword

- An enterprise network may often consist of a substantial number of host devices, each requiring network parameters in the form of IP addressing and additional network configuration information. Manual allocation is often a tedious and inaccurate business which can lead to many end stations facing address duplication or failure to reach services necessary for smooth network operation. DHCP is an application layer protocol that is designed to automate the process of providing such configuration information to clients within a TCP/IP network. DHCP therefore aids in ensuring correct addressing is allocated, and reduces the burden on administration for all enterprise networks. This section introduces the application of DHCP within the enterprise network.

# Objectives

- Upon completion of this section, you will be able to:
  - Describe the function of DHCP in the enterprise network.
  - Explain the leasing process of DHCP.
  - Configure DHCP pools for address leasing.

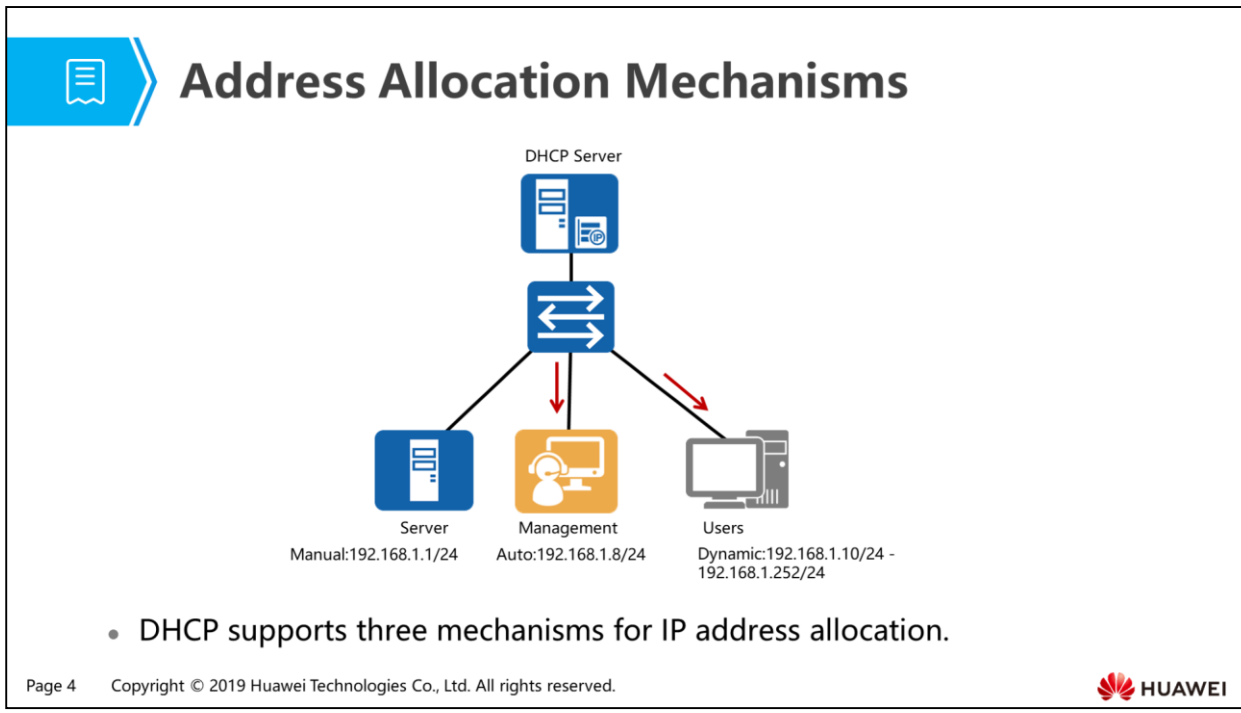
## DHCP Application In The Enterprise Network




- Networks comprising of a large number of users requires a central management system for IP address allocation.

- Enterprise networks are often comprised of multiple end systems that require IP address assignment in order to connect with the network segment to which the end system is attached. For small networks, a minimal number of end systems attached to the network allows for simple management of the addressing for all end systems.
- For medium and large-scale networks however, it becomes increasingly difficult to manually configure IP addresses with increased probability of duplication of addressing, as well as misconfiguration due to human error, and therefore the necessity to implement a centralized management solution over the entire network becomes ever more prominent. The Dynamic Host Configuration Protocol (DHCP) is implemented as a management solution to allow dynamic allocation of addresses for existing fixed and temporary end systems accessing the network domain.
- In cases it is also possible that there may be more hosts than available IP addresses on a network. Some hosts cannot be allocated a fixed IP address and need to dynamically obtain IP addresses using the DHCP server. Only a few hosts on a network require fixed IP addresses.




- DHCP supports three mechanisms for IP address allocation. The method of automatic allocation involves DHCP assigning a permanent IP address to a client. The use of dynamic allocation employs DHCP to assign an IP address to a client for a limited period of time or at least until the client explicitly relinquishes the IP address.
- The third mechanism is referred to as manual allocation, for which a client's IP address is assigned by the network administrator, and DHCP is used only to handle the assignment of the manually defined address to the client. Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily, or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses.
- Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network, where IP addresses are sufficiently scarce that addresses are able to be reclaimed when old clients are retired. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses in environments where it may be more desirable to meticulously manage IP address assignment.

# DHCP Messages

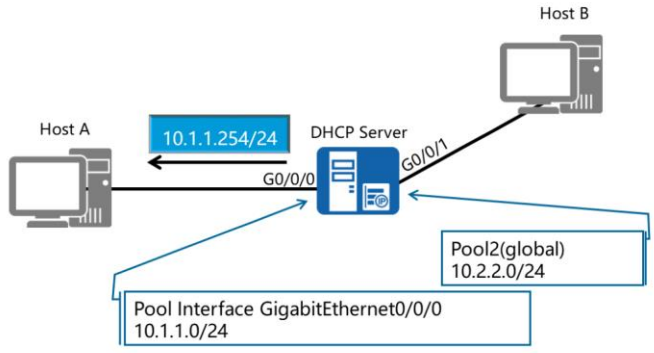
| Message Types | Function |
|---|---|
| DHCP DISCOVER | Client broadcast used to locate available DHCP servers. |
| DHCP OFFER | Server responds to DHCPDISCOVER with an offer of configuration parameters. |
| DHCP REQUEST | Client message to servers, either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming the correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address. |
| DHCP ACK | Server confirmation sent to the client with configuration parameters, including committed network address. |
| DHCP NAK | Server indicates to the client that client's requested network address cannot be assigned. |
| DHCP RELEASE | Client relinquishes the network address to the server and cancels the remaining lease. |





- A DHCP server and a DHCP client communicate with each other by exchanging a range of message types. Initial communication relies on the transmission of a DHCP Discover message. This is broadcast by a DHCP client to locate a DHCP server when the client attempts to connect to a network for the first time. A DHCP Offer message is then sent by a DHCP server to respond to a DHCP Discover message and carries configuration information.
- A DHCP Request message is sent after a DHCP client is initialized, in which it broadcasts a DHCP Request message to respond to the DHCP Offer message sent by a DHCP server. A request message is also sent after a DHCP client is restarted, at which time it broadcasts a DHCP Request message to confirm the configuration, such as the assigned IP address. A DHCP Request message is also sent after a DHCP client obtains an IP address, in order to extend the IP address lease.
- A DHCP ACK message is sent by a DHCP server to acknowledge the DHCP Request message from a DHCP client. After receiving a DHCP ACK message, the DHCP client obtains the configuration parameters, including the IP address. Not all cases however will result in the IP address being assigned to a client. The DHCP NAK message is sent by a DHCP server to in order reject the DHCP Request message from a DHCP client when the IP address assigned to the DHCP client expires, or in the case that the DHCP client moves to another network.
- A DHCP Decline message is sent by a DHCP client, to notify the DHCP server that the assigned IP address conflicts with another IP address. The DHCP client will then apply to the DHCP server for another IP address.
- A DHCP Release message is sent by a DHCP client to release its IP address. After receiving a DHCP Release message, the DHCP server assigns this IP address to another DHCP client.
- A final message type is the DHCP Inform message, and is sent by a DHCP client to obtain other network configuration information such as the gateway address and DNS server address after the DHCP client has obtained an IP address.

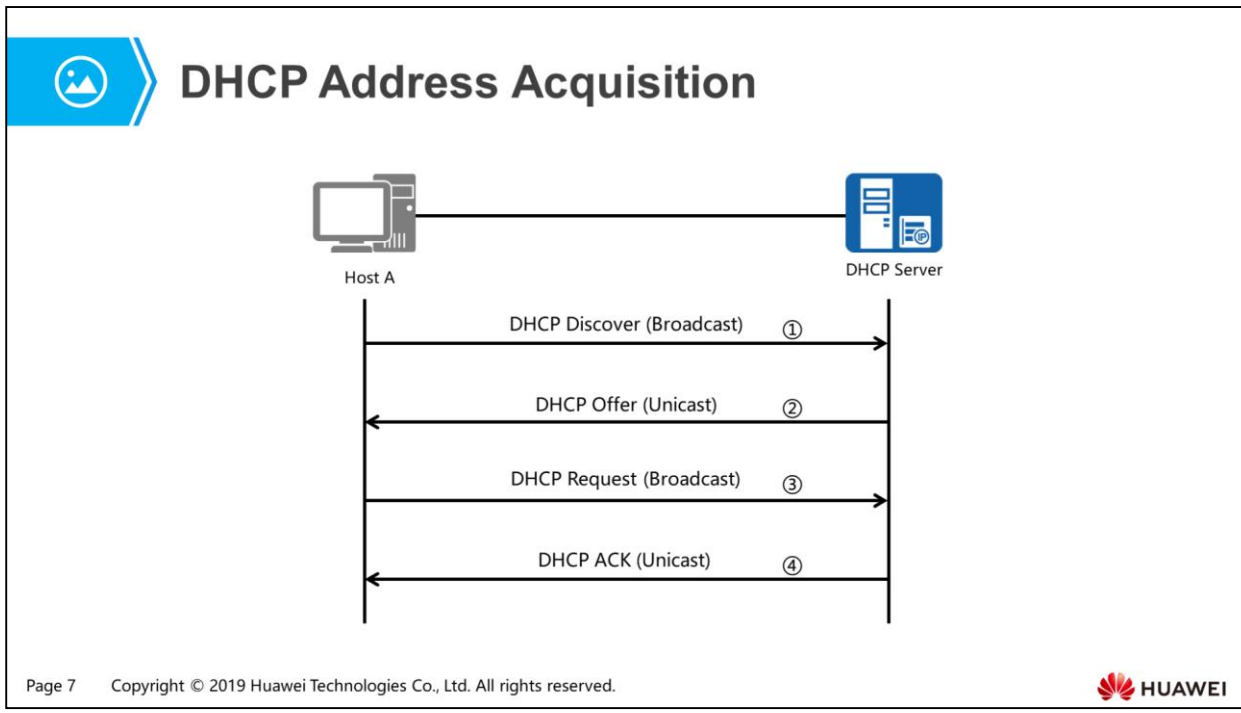
# Address Pools




- Address pools can be either global or interface based.

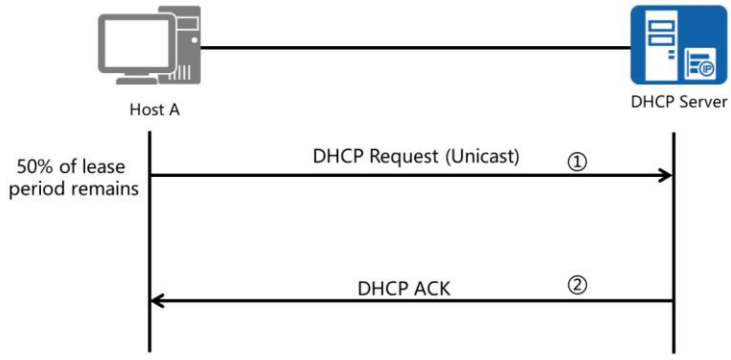
 

- The AR2200 and S5700 series devices can both operate as a DHCP server to assign IP addresses to online users. Address pools are used in order to define the addresses that should be allocated to end systems. There are two general forms of address pools which can be used to allocate addresses, the global address pool and the interface address pool.
- The use of an interface address pool enables only end systems connected to the same network segment as the interface to be allocated IP addresses from this pool. The global address pool once configured allows all end systems associated with the server to obtain IP addresses from this address pool, and is implemented using the dhcp select global command to identify the global address pool. In the case of the interface address pool, the dhcp select interface command identifies the interface and network segment to which the interface address pool is associated.
- The interface address pool takes precedence over the global address pool. If an address pool is configured on an interface, the clients connected to the interface obtain IP addresses from the interface address pool even if a global address pool is configured. On the S5700 switch, only logical VLANIF interfaces can be configured with interface address pools.




- The acquisition of an IP address and other configuration information requires that the client make contact with a DHCP server and retrieve through request the addressing information to become part of the IP domain. This process begins with the IP discovery process in which the DHCP client searches for a DHCP server. The DHCP client broadcasts a DHCP Discover message and DHCP servers respond to the Discover message.
- The discovery of one or multiple DHCP servers results in each DHCP server offering an IP address to the DHCP client. After receiving the DHCP Discover message, each DHCP server selects an unassigned IP address from the IP address pool, and sends a DHCP Offer message with the assigned IP address and other configuration information to the client.
- If multiple DHCP servers send DHCP Offer messages to the client, the client accepts the first DHCP Offer message received. The client then broadcasts a DHCP Request message with the selected IP address. After receiving the DHCP Request message, the DHCP server that offers the IP address sends a DHCP ACK message to the DHCP client. The DHCP ACK message contains the offered IP address and other configuration information.
- Upon receiving the DHCP ACK message, the DHCP client broadcasts gratuitous ARP packets to detect whether any host is using the IP address allocated by the DHCP sever. If no response is received within a specified time, the DHCP client uses this IP address. If a host is using this IP address, the DHCP client sends the DHCP Decline packet to the DHCP server, reporting that the IP address cannot be used, following which the DHCP client applies for another IP address.

## DHCP Lease Renewal



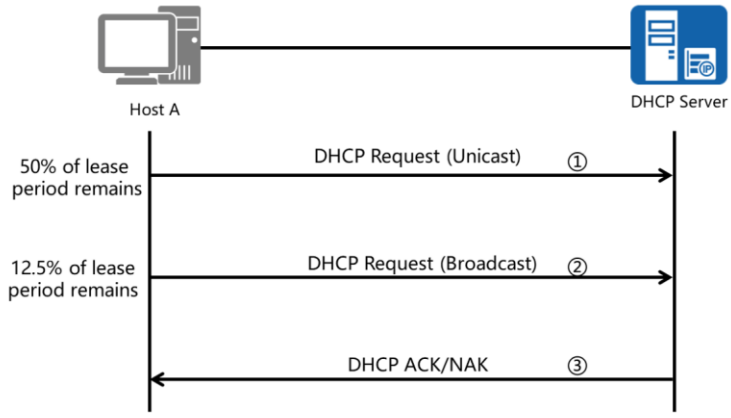

- DHCP initiates an IP lease renewal process when a lease period of 50% remains.



HUAWEI

- After obtaining an IP address, the DHCP client enters the binding state. Three timers are set on the DHCP client to control lease update, lease rebinding, and lease expiration. When assigning an IP address to a DHCP client, a DHCP server specifies values for the timers.
- If the DHCP server does not set the values for the timers, the DHCP client uses the default values. The default values define that when 50% of the lease period remains, the release renewal process should begin, for which a DHCP client is expected to renew its IP address lease. The DHCP client automatically sends a DHCP Request message to the DHCP server that has allocated an IP address to the DHCP client.
- If the IP address is valid, the DHCP server replies with a DHCP ACK message to entitle the DHCP client a new lease, and then the client re-enters the binding state. If the DHCP client receives a DHCP NAK message from the DHCP server, it enters the initializing state.

## DHCP Rebinding Expiry



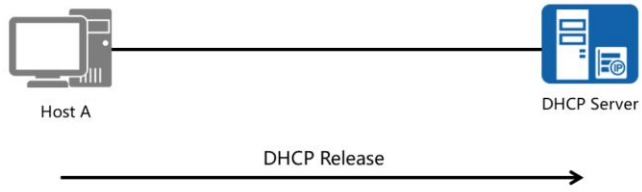

- Rebinding will occur if the lease is not renewed in time.





- After the DHCP client sends a DHCP Request message to extend the lease, the DHCP client remains in an updating state and waits for a response. If the DHCP client does not receive a DHCP Reply message from the DHCP server after the DHCP server rebinding timer expires which by default occurs when 12.5% of the lease period remains, the DHCP client assumes that the original DHCP server is unavailable and starts to broadcast a DHCP Request message, for which any DHCP server on the network can reply with a DHCP ACK or NAK message.
- If the received message is a DHCP ACK message, the DHCP client returns to the binding state and resets the lease renewal timer and server binding timer. If all of the received messages are DHCP NAK messages, the DHCP client goes back to the initializing state. At this time, the DHCP client must stop using this IP address immediately and request a new IP address.

# IP Address Release

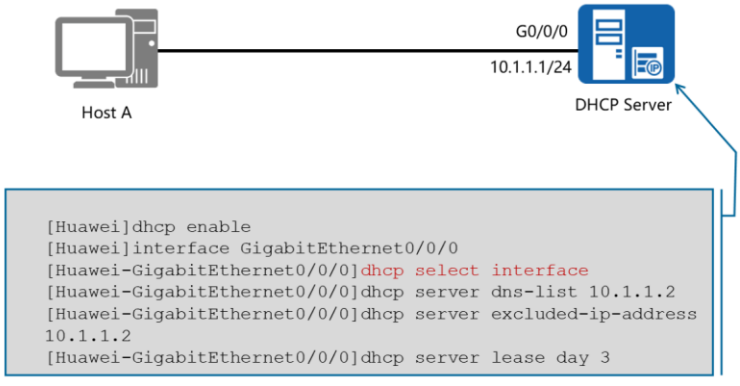



- DHCP will result in the release of an IP address if the client fails to renew the IP address before the lease expiry.

  HUAWEI

- The lease timer is the final timer in the expiration process, and if the DHCP client does not receive a response before the lease expiration timer expires, the DHCP client must stop using the current IP address immediately and return to the initializing state. The DHCP client then sends a DHCP DISCOVER message to apply for a new IP address, thus restarting the DHCP cycle.

## DHCP Interface Pool Configuration




```
[Huawei]dhcp enable
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address
10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3
```

  HUAWEI

- There are two forms of pool configuration that are supported in DHCP, these include defining a global pool or an interface based pool. The *dhcp select interface* command is used to associate an interface with the interface address pool in order to provide configuration information to connected hosts. The example demonstrates how interface Gigabit Ethernet 0/0/0 has been assigned as part of an interface address pool.