Routing

1. Overview: layering, routed versus routing protocols, switching and routing, IP addressing.

All	Application	Data	Don’t
People	Presentation	Data	Don't
Seem	Session	Data	Don't
To	Transport	Segments	Stop
Need	Network	Packets	Pouring
Domino's	Data-link	Fragments	Free
Pizza	Physical	Bits	Beer

Routing protocols distribute routing information throughout all routers on a network. OSPF, RIP, EIGRP or BGP.

A **routed** protocol is a layer 3 **protocol (TCP/IP)** that routes data and applies logical addresses to devices.
It's being **routed** through different networks.

Routing protocol **provides** information**. Routed** protocol **uses** this information

Switches create a network. Routers connect networks.

Switching packets **inside** the subnet > **MAC Addresses** (Mac table) on **Layer 2.** (48 bits)
Routing - routes packets **between** the subnets, inside the BIG network > **IP Addresses** on **Layer 3.**
Using the network ID/Destination comparing it to the routing table on Layer 3 (more **intelligent** switching)

Source and destination IP stay the **same** the entire life of a packet (in general), but MAC addresses are **re-written** every time they pass through a **router**.
To put it in its simplest terms, devices on one network will **NOT** learn the MAC address of devices on another network.

You really need to have the OSI model in mind and the encapsulation that's done and what's added in each Layer in the **PDU**(Protocol Data Unit).

PC1 **ANDING** PC2's IP addr. And it's SM to see if they are on the same subnet. If not - PC1 sends the data to R1(gateway), if it doesn't have the MAC in its ARP, it will do ARP and then send the data. R1 receives the data, checks if the packet is for him > DEST IP != R1 IP > check routing table for DEST IP ? > If he has a route, he sends it to R2 (next hop), if he hasn't - he does ARP and then forwards. R2 does the same and forwards it to PC2.
SRC/DEST IP stays the same, but SRC/DEST MAC changes!

IP Addressing:

Internet Protocol (**IP**) provides two fundamental Network layer services:
Logical Addressing - provides unique address (network id + host id)
Routing - determines the best path to destination and routes data accordingly

Hardware address: HARDCODED ! used to uniquely identify a host within a local network. Function of the **Data-Link (Layer 2)**.

Ethernet uses Media Access Control (MAC) = 48 bits (hex), first SIX hex digits = **manufacturer**, the last SIX = **host ID**

>> L2 network just by switches = flat network, no hierarchy = ENORMOUS broadcast domain

The scalability limitations of Layer-2 hardware addresses are mitigated using logical addresses.
Logical Address: Network Layer 3 and provides hierarchy, not hardcoded, but CAN BE **dynamically** assigned and changed.
Two components: **Network ID + Host ID (+ SubnetMask** which identifies the network)
32 bits = 4 Octets!
Hosts on different networks require a **router** to communicate:

Host A: 158.**80**.164.100 255.255.0.0
Host B: 158.**85**.164.101 255.255.0.0

IP Address Classes:

Class A	1 - 127	255.0.0.0	127 Net	16.777.214 Hosts	0xxx

Class B	128 -191	255.255.0.0	16384 Net	6534 Hosts	10xx
Class C	192 - 223	255.255.255.0	2097152 Net	254 Hosts	110x
Class D	224 - 239	**Multicast**	**Traffic**	**-**	1111

Too much useful addresses are lost due to the lack of flexibility!!!

On each IP network, **two** host addresses are reserved for special use:
Network address (usually the **first** address of the spectrum). It's used in routing tables and contains all **0** in the host portion.
Broadcast address (usually the **last** address of the spectrum). == all hosts on the network. Contains all **1** in the host portion.
Router **never** forwards a multicast or broadcast packet from on interface to another
Switch **always** forwards multicast or broadcast packets to every port, except the original port the signal came from

Subnetting is the process of stealing bits from the host portion of the subnet mask. **More** hosts = **less** networks.

To get 10 new network we need 2^n >= 10 > 2^4 = 16 networks > we need to steal 4 bits from the hosts octet > 255.255.255.**240 or /28** (24+4)
2^4 = 16 - 2 = 14 available hosts per network
0.0.0.0/0 - reserved to identify all networks **= default route**.
Magic Number: last borrowed BIT = network increment - number of borrowed bits > 2 * n = number of subnets
Next > 2^n -2 = usable hosts

==

2. Overview: IP addressing, VLSM (Variable Length Subnet Mask) and CIDR (Classless Inter-Domain Routing).

CIDR (Classless Inter-Domain Routing) - simplified method of representing a subnet mask. CIDR identifies the number of bits set to 1 (on) preceded by a slash. 192.168.1.1/24 or /30 ...

VLSM allows the use of different masks for each subnet. After a network address is subnetted, those subnets can be further subnetted. VLSM is simply subnetting a subnet. VLSM can be thought of as sub-subnetting.
Subnetting 10.0.0.0/8 to 10.0.0.0/16, /16 to /24...

==

3. Introduction to Routing and Packet Forwarding

Routing is the process of forwarding packets of information from one **network** to another. Therefore routes are based on the destination **network**, and NOT the destination host. The routing decisions are based on a routing table (Destination IP is checked against the routing table). If there is no route in the table, they will send the packet to the **default gateway**.
Routers deal with **networks. Switches** deal with **hosts!**

Routing tables contain:
The **destination** network and its **subnet mask**
The "**next hop**" router to the destination network
Routing **metrics** and **administrative distance (AD)**

To determine the best route to a destination, elements are considered in the following order:

Prefix length - number of bits used to identify the network (the more, the better) > ***ALWAYS PREFERRED !***

Metric (within a routing protocol) - **Distance** vs **Cost**

Administrative distance (between separate routing protocols) **EIGRP = 90; OSPF = 110; RIP = 120**

Only routes with the **best metric** are **added** to the routing table. If rotes have the same metric, most protocols will **load-balance**

If a router is running multiple routing protocols, **Administrative Distance** is used to determine which one is to be trusted.(Lower = better).

Connected	0
Static	1
EIGRP Summary	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115

RIP	120
External EIGRP	170
Internal BGP	200
Unknown	**255**

Unknown is never inserted!

Router# *show ip route* --show the routing table

[120/1] = 120 = 120 AD; 1 = hop-count

Router# *clear ip route** --clear the table, force the protocols to repopulate it

===

4. Static Routing. Default Routes and On-Demand Routing.

A static routing table is created, maintained and updated by a network administrator **MANUALLY**.

A static route to every network must be configured on **EVERY** router for full connectivity. This provides superior **control** over routing, but quickly becomes impractical on large networks. Also **DOES NOT** adapt to network changes > more work

Routers will **NOT share STATIC** routes thus reducing CPU/RAM overhead and saving bandwidth.

Static routes have an **AD of 1** and are always preferred over dynamic routes, UNLESS the default **AD** is changed.

A static route with an **adjusted AD** is called a **floating static route** serving as a **backup** to a static route. s

A dynamic routing table is created, maintained and update by a ROUTING protocol running on the router (RIP, EIGRP, OSPF)

Routers SHARE dynamic routing information with each other, thus increasing CPU and RAM and bandwidth usage. They are capable of dynamically choosing a different (better) path in case the network changes.

Static routing: Advantages: minimal CPU/RAM overhead; no bandwidth overhead (updates are not shared); better control on routes

Disadvantages: changes have to be manually configured; no dynamic changes; impractical on large scale

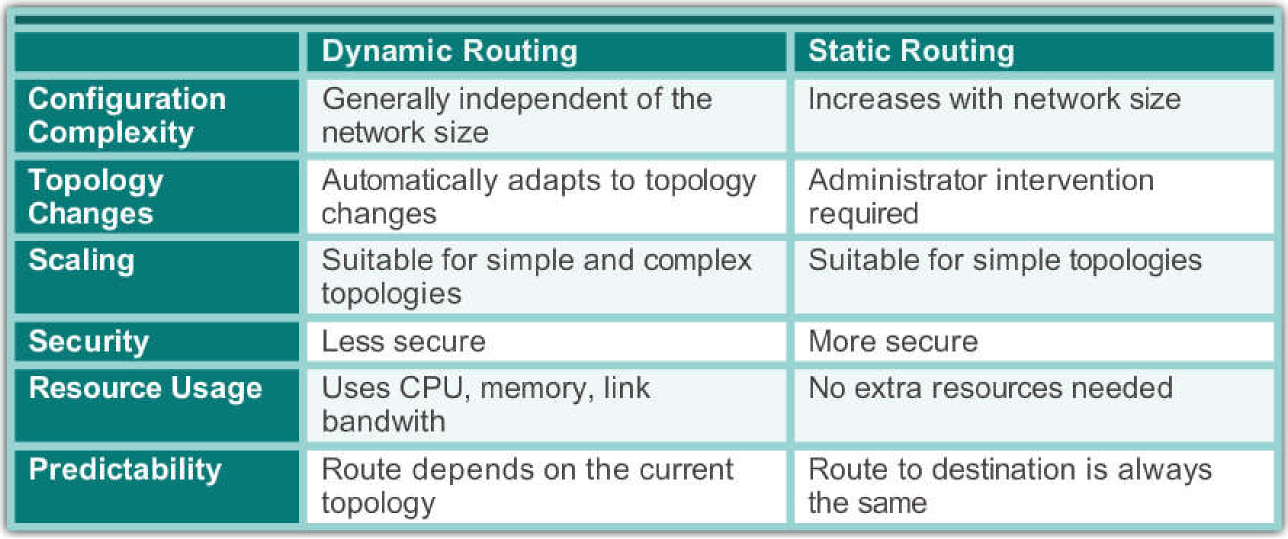
Dynamic routing: Advantages: simpler to configure on large scale; dynamically chooses a new/better path; **can load balance**

Disadvantages: updates are shared - consume resources; calculations put load on CPU/RAM; no strict choice of best route

On-Demand Routing:

ODR (On Demand Routing) is designed to be used in a partially meshed environment (e.g Frame Relay networks) where a hub router maintains one link each to multiple stub routers (spokes routers). Therefore, for any spoke to communicate with another spoke, such traffic must pass through the hub.

On-Demand Routing (ODR) is an enhancement to **Cisco Discovery Protocol** (**CDP**), a protocol used to discover other Cisco devices on either broadcast or non-broadcast media. With the help of CDP, it is possible to find the device type, the IP address, the Cisco IOS® version running on the neighbor Cisco device, the capabilities of the neighbor device, and so on. ODR is able to carry Variable Length Subnet Mask (VLSM) information.



	Dynamic Routing	Static Routing
Configuration Complexity	Generally independent of the network size	Increases with network size
Topology Changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource Usage	Uses CPU, memory, link bandwith	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

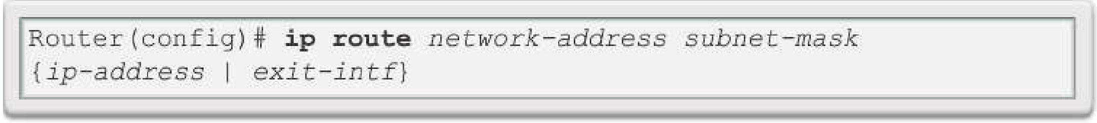
===

5. A Routing Table.

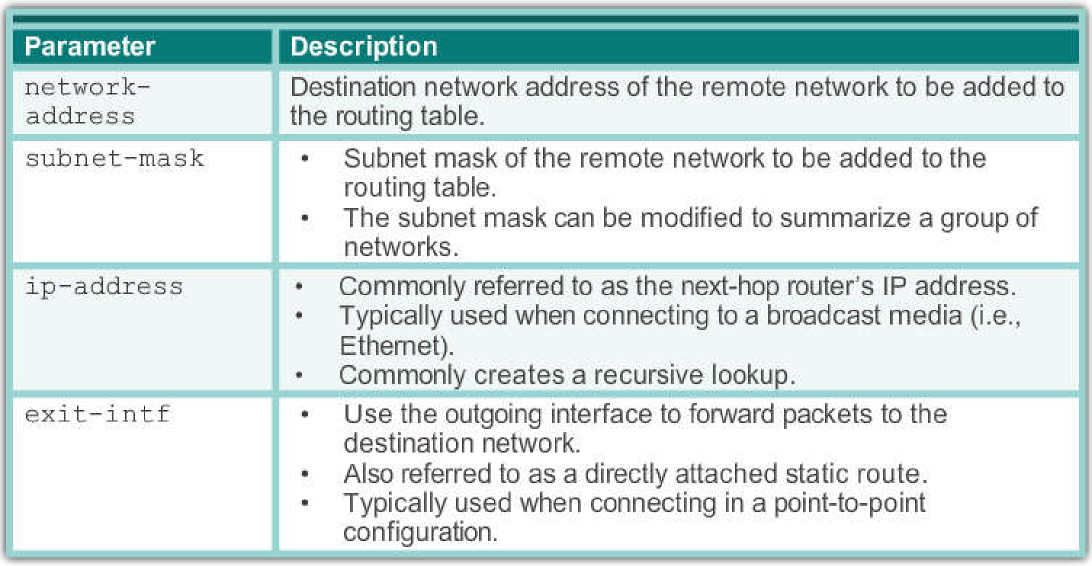
There are two common types of static routes in the routing table:

- Static route to a specific network
- Default static route = default gateway **ip route 0.0.0.0 0.0.0.0**{*exit-intf* | *next-hop-ip*}

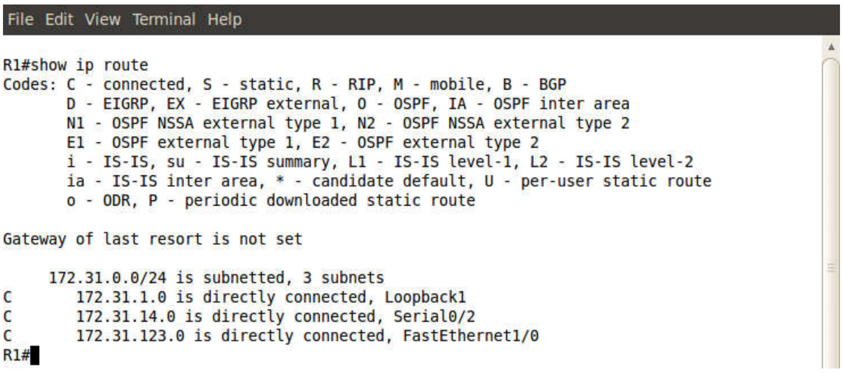
S = static route; * = possible default route



```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```



Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table.
subnet-mask	• Subnet mask of the remote network to be added to the routing table. • The subnet mask can be modified to summarize a group of networks.
ip-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/24 is subnetted, 3 subnets
C       172.31.1.0 is directly connected, Loopback1
C       172.31.14.0 is directly connected, Serial0/2
C       172.31.123.0 is directly connected, FastEthernet1/0
R1#
```

Route Summarization:

It's meant to make the job of the router easier. **Less processing** needed to determine a route for a packet. But with modern CPUs in routers, it really isn't an issue.

The only benefit besides that is possibly **easier** to **read routing** tables, but that's **arguable**. With auto summary you can also have two groups of similar classless subnets on each side of a network, and when summarized to their classful boundaries, end up overlapping each other and causing a routing conflict/loop.

==

6. Introduction to Dynamic Routing Protocols. ***Route Filtering ?***. Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). Distance Vector versus Link State Routing Protocols.

Distance-vector protocols - RIP, IGRP - uses **distance**

- Two factors: **distance** or **metric** to the destination, and the **vector** - **direction**.
- Each node knows only about the **next hop**, this leads to poor decisions if a link is DOWN somewhere. False routing until the protocol re-converges.
- Routing information is exchanged only by directly connected routers (full routing table) = **ROUTING BY RUMOR.**
- **Anti-loop**:

- **Route poisoning** - sending an update about an unreachable route marking its Hopcount = 16 = unreachable. HOLD DOWN TIMER starts, not updating the router until and update is received from the same router, about the same route.
    - **Poison-reverse** - after receiving poisoning, the router sends an update back. This is to ensure that all routers on a segment have received the poisoned route information.
- **Split-Horizon** - prohibits a router from advertising a router back to the interface from which it was learned. **(ADDS DIRECTION?)**

Less overhead vs Limited visibility.

Link-state protocols - OSPF, IS-IS - uses **cost**

- Each node has a **complete** understanding of the **topology**, thus if a link fails, each node can re-calculate the new route. Each node has to have a complete view of the topology.
- **Neighbor relations > LSA > Topology/Link-state DB > Algorithm > shortest path!**

More overhead + robustness & scalability.

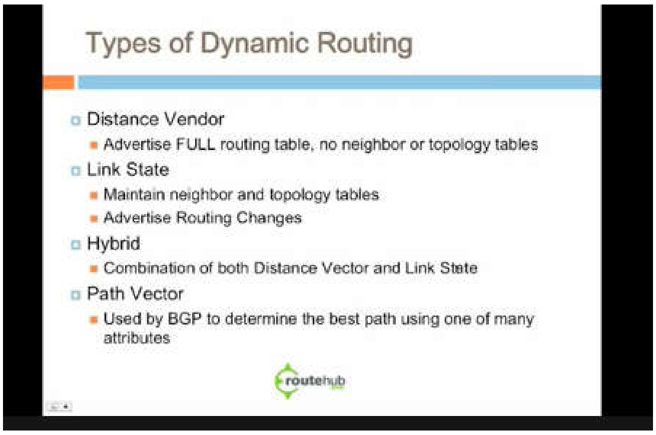
EIGRP = HYBRID! - Forms **neighbor** relationships + vectors and send **only partial** and **triggered** updates

EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. For example, EIGRP doesn't send link-state packets as OSPF does; instead, **it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router**. And EIGRP has link-state characteristics as well—it synchronizes routing tables between neighbors at startup and then sends specific updates only when topology changes occur. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255 (the default is set to 100).

Interior Protocols: within **AUTONOMOUS SYSTEM** (subnets under the control of a single administrative entity and the same routing policy)

Exterior Protocols: are used for exchanging routing information between **AUTONOMOUS SYSTEMS**, such as Border Gateway Protocol.

They rely on IGPs to resolve routes within an AS



Types of Dynamic Routing

- Distance Vendor
    - Advertise FULL routing table, no neighbor or topology tables
- Link State
    - Maintain neighbor and topology tables
    - Advertise Routing Changes
- Hybrid
    - Combination of both Distance Vector and Link State
- Path Vector
    - Used by BGP to determine the best path using one of many attributes

==

7. Distance-Vector Routing Protocols.

Use **distance/hop count** as their metric: how routers away is the network. **Where and how far**?

RIP, IGRP

Periodic updates of the **full** routing table are sent to routing **neighbors**

Distance-vector protocols suffer from slow convergence and are prone to loops

Some form of 'distance' is used to calculate a route's metric.

Bellman-Ford algorithm is used to determine the shortest path

A distance-vector routing protocol begins by advertising directly-connected networks to its neighbors.

RIP - every **30** sec; IGRP - every **90** sec. Each neighbor adds the routes from the updates to their routing table, they trust the update **completely**, and will forward their routing table (connected and learned routes) to every other neighbor. **Routing by rumor**.

They send their routing tables, received updates are compared and the differences are added to their routing tables.

Because of the **periodic** updates, **distance-vector** protocols converge **slowly.** Also, trusting **blindly** their neighbors, they are highly **susceptible** to **routing loops.**

Distance-vector protocols utilize some form **of distance** to calculate a route's metric.

RIP uses **hop-count. IGRP** uses a composite of **bandwidth and delay.**

==

8. Link-State Routing Protocols.

Use **cost** as their metric: **OSPF, IS-IS**

SHARES only link info individually!

Link-state routing protocols were developed to alleviate the **convergence** and **loop issues** of **distance-vector** protocols.

They maintain three separate tables:

- **Neighbor table** - contains a list of all neighbors, and the interface each neighbor is connected to.

  Neighbors are formed by sending **Hello** packets.
- **Topology table** - otherwise known as the **link-state** table - contains a map of all links within an **area,** including each link's status.
- **Shortest-path table** - contains the best routes to each particular destination (a.k.a. **routing table**)

Link-state protocols do NOT 'route by rumor' - they send updates advertising the **state** of their links. (**link** being a directly connected network). All routers know the state of all existing links in their **area** and store this information in a **TOPOLOGY** table.

All routers within an area have *identical* topology tables.

The best route to each link (network) is stored in the **shortest-path (routing) table**. If the state of a link changes (interface failing), and advertisement containing **ONLY this link-state change** will be sent to all routers in the **area.** Each router will adjust its **topology** table accordingly and will calculate a new **best** route if required.

Consistent **topology tables** means **link-state** protocols can CONVERGE very quickly and are IMMUNE to routing loops.

Also, because updates are sent only after link-state changes, and contain only the change, they are LESS bandwidth-intensive, than distance-vector protocols.

However, the three **tables** utilize more **resources** on the router itself.

For the metric, the **Dijkstra formula** is used to determine the shortest path.

==

9. Routing Information Protocol

RIP (Routing Information Protocol) is a standardized Distance Vector protocol, designed for use on smaller networks, and is widely supported.

Timers: (ALSO VALID FOR RIPv2) !!!

Update Timer - **30** seconds (default) - sending updates to **BROADCAST (v1) or MULTICAST (v2)**

Invalid Timer - **180** seconds - how long a route remains in the routing table before marked as ***invalid*** if no updates are heard about this route. If an update is received, the timer is restarted. **INVALID = 16 METRIC = UNREACHABLE.**

Hold-down Timer - **180** second - routes in **hold-down** state:

- **Invalid** timer has expired
- Marked with **metric 16** from another update
- Marked with a **higher metric** from another update to prevent loops

Flush Timer - **240** seconds - runs with **Invalid timer** - flushed **60 secs** after marked invalid.

Timers have to be identical on all routers!!!

SLOW CONVERGENCE, because the update has to **HOP** through every connected router!

PASSIVE INTERFACES: disable MULTICAST updates FROM specific interface, but listen to INCOMING updates (if there are just end devices beyond that)

# passive-interface s0

# passive-interface default //all are passive

# no passive-interface s0 //just s0 is not passive

RIP Neighbors: RIP sends updates AS **BROADCAST; RIPv2 AS MULTICAST 224.0.0.9 !**

We can configure RIP ***neighbors***, which allow **unicast** routing to those neighbors.

> # neighbor 10.3.5.1

BUT, the router will still **broad/multicast** in addition to the **unicast,** therefore we need passive interfaces!

>\# passive-interface s0

```
>#neighbor 10.3.5.1
```

Interoperating RIP and RIPv2 (**PER INTERFACE BASIS)**

```
># interface s0
># ip rip send version 2; #ip rip receive version 1; #ip rip receive version 1 2; #ip rip v2-broadcast
```

Only **on p2p** send update only on change:

- `># ip rip triggered`

Debugging:

```
># show ip route (opt. 172.18.0.0); # show ip protocols (rip timers, versions..); #
```

Router 0# default information originate //shares the static routes (0.0.0.0!!!)

==

9.1 .RIP version 1.

>> Does NOT support VLSM! >> networks must be contiguous. (same major network & subnetmask

Characteristics: periodic router updates - **30 seconds -** as broadcasts to 255.255.255.255

send out the **full routing table** every update

it's metric is the **hopcount, max hopcount = 15 hops**

Bellman-Ford algorithm for determining the best 'path'

AD = 120

can load balance up to 4 paths with **equal metric (hopcount)** > slower links can congest

==

10. RIPv2.

RIPv2 is classless! **>> includes SM into updates > networks can be discontiguous.**

Enhancements in v2: Updates are sent via **multicast 224.0.0.9**

Encrypted authentication can be configured between routers

Route tagging is supported - allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.

RIPv2 can work with RIPv1:

V1 sends only **V1** packets

V1 receives both **v1** and **v2** updates

V2 sends both v1 and v2 updates , but receives **ONLY V2 updates**

Unless RIPv2 is manually specified, Cisco will **default** to **RIPv1** when configuring RIP.

Configure RIPv1:

Router(config)# router rip *//enables the RIP process*

Router(config)# network 172.16.0.0 *//which networks we wish to advertise to other routers*

Router(config)# network 172.17.0.0 *//they are the networks directly connected*

==

11. Hybrid Routing Protocols. **EIGRP (Enhanced Interior Gateway Routing Protocol).**

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

Works with AS number! # *router eigrp 10 //for AS 10*

Metric: Bandwidth and **Delay** of the Line are used! [10000000/bandwidth+delay]*256

CISCO Proprietary protocol. **HYBIRD!!! Fast Convergence!**

Support VLSM.

Can run multiple protocols >> Reliable Transport Protocol !!!

RTP > supports reliable and unreliable !

Load balancing - equal or not-equal paths.

Authentication - Router ID

Note: Only EIGRP supports **unequal** cost load balancing.

Diffusing Update Algorithm (DUAL) - determines the best path and ensures loop free routing, also **backup** routes!!!

EIGRP forms **neighbor** relations with adjacent routers in the same **AS.** >> **Neighbor Table** >> **Hello Timers** to keep alive

Updates are sent either by **UNCIAST or MULTICAST(224.0.0.10)** by **Reliable Transport Protocol**

Updates are sent **ONLY** when a change occurs and **ONLY** the change (Bounded Triggered Updates)

Cost = Bandwidth + Delay of the line

HOLD TIMER: how long the router waits before marking the route inactive, if it stops receiving hello packets

By default: 3 x Hello Timer, can also be adjusted per interface, and must not be the same on All routers.

Neighbor Table - IP of the router, Interface from which the HELLO came, Hold timer, sequence number

Adjacencies will not form unless the primary IPs are on the same subnet

Topology Table - saves a backup path - list of **ALL** routes in the AS

Routing Table - the best route for each known network

Packets:

Hello - unreliable ; multicast - form neighbor relationships; **5 secs** on fast, **60 secs** on slow links

Update - reliable; unicast(for new neighbors) or multicast (if a metric is changed)

Query - reliable; unicast or multicast - when a **Successor** route fails, and there are not **FS**, the route is in **active** state and **queries** for an alternative route.

Reply - reliable ; unicast - response to **query** - only with an alternative route **(???)**

ACK - unreliable ; unicast - acknowledges delivery - **HELLO** packets with NO DATA, just an ACK number

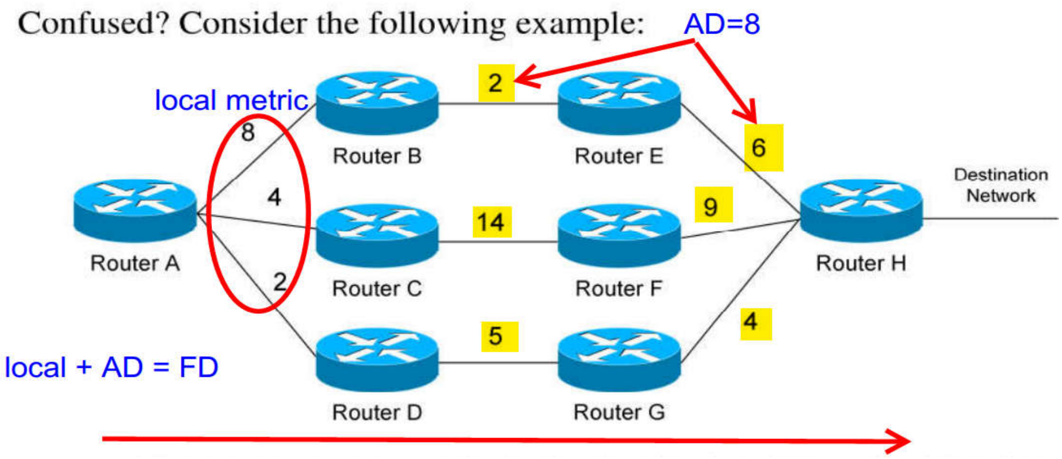
Router updates, containing all known routes and their metrics, populate the TOPOLOGY table. The router with the lowest metric will be the ~~feasible distance~~ **chosen** and will be installed into the table.

Feasible distance = advertised distance (from the other router to the network) + the metric to the router itself

To converge quickly, the topology table contains also **feasible successors.** The successor's **advertised distance** Has to be less than the current **feasible distance.** This is known ad the **Feasible condition (FC).**

Routes that are not **feasible successors** become route **possibilities.**

Successors allow the routers to provide connectivity without reconverging.



We'd have 3 FDs:

8 + (2 + 6) = **16 << Feasible Successor**

4 + (14 + 9) = **27 << Possbilitiy**

2 + (5 + 4) = **11** << **Smallest** goes into the table!

If no Feasible Successor exists and a link fails, a route will enter an **Active** (converging) state until an alternate route is found.

Router# *show ip eigrp topology (active) // only active*

(all-links) //all links

Passive Interfaces: but the interface will **neither SENT** nor **RECEIVE** updates or hello packets (>> no NEIGHBOR relations!!)

#passive-interface s0 //only s0 passive

#passive-interface default //every is passive

#no passive-interface s0 //only s0 will NOT be passive

Router 0# redistribute static //shares the static routes (0.0.0.0!!!)

Useful:

#show eigrp neighbors

#show eigrp interfaces // which interfaces have eigrp

===

12. OSPF.

Separates an **Autonomous System** into individual **areas** !!!

Routers build a **Topology Database** of all links **within** their area, all routers **within the same area** have identical topology DBs.

Updates contain only information about local links. >> **CONSERVES** bandwidth and CPU load.

Area 0 = BACKBONE - all others areas must connect to **Area 0,** or use **virtual links to it.**

Adjacent router's interfaces have to be in the **same area** to form a neighbor relationship and share updates!

Link-State protocol, scales efficiently to support larger networks

Loopback interfaces = ALWAYS UP!

== Router ID = ALWAYS THE SAME! Can be every X.X.X.X ID e.g. 200.200.200.200 (it's also high)

Process ID can be different on every router!

Link State Advertisement - update, explain something to someone

Support multiple areas! == group of routers

Authentication!

Shortest Path First Algorithm

Complex **cost** calculation! With many features!

Databases:

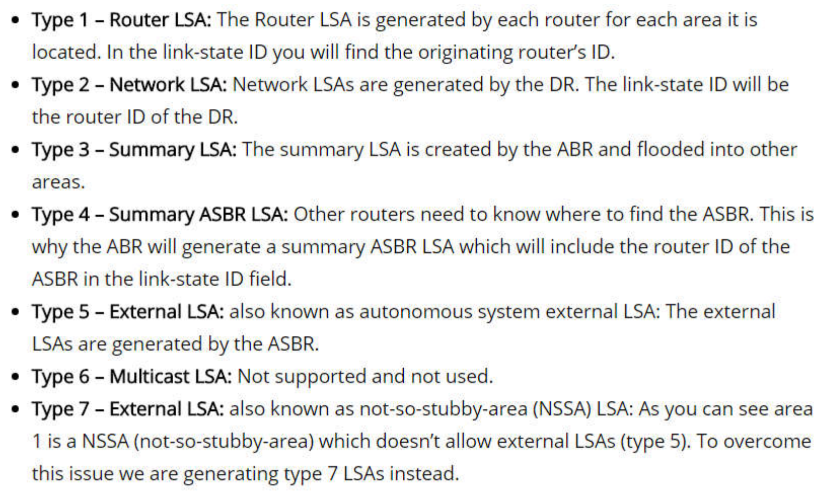
- Adjacency - Neighbors - say hello to them, share info = establish connection to the neighbors and keep it up
- Link-state - Topology table -
- Forwarding - SPF runs against the Link-State table and populates this one and then the routing table

Packets:

  - **Hello**, **10 secs**, **30** on Frame Relay @ 224.0.0.5 < built in Dead Timer
- Database description - Link-State DB ChecK
- Link-State **Request** - request more info on an entry
- Link-State **Update** - reply to a request/update after change
- Link-State **Ack.** - acknowledges an update "thx I got it"

Learns first about the:

1. **Directly** connected ?
2. Hello Packets to adjacencies
3. Build Link-State Packets
4. Flood LSP Neighbors
5. Collects LSP's and builds topology map
6. Run SPF and populate the routing table



- **Type 1 – Router LSA:** The Router LSA is generated by each router for each area it is located. In the link-state ID you will find the originating router's ID.
- **Type 2 – Network LSA:** Network LSAs are generated by the DR. The link-state ID will be the router ID of the DR.
- **Type 3 – Summary LSA:** The summary LSA is created by the ABR and flooded into other areas.
- **Type 4 – Summary ASBR LSA:** Other routers need to know where to find the ASBR. This is why the ABR will generate a summary ASBR LSA which will include the router ID of the ASBR in the link-state ID field.
- **Type 5 – External LSA:** also known as autonomous system external LSA: The external LSAs are generated by the ASBR.
- **Type 6 – Multicast LSA:** Not supported and not used.
- **Type 7 – External LSA:** also known as not-so-stubby-area (NSSA) LSA: As you can see area 1 is a NSSA (not-so-stubby-area) which doesn't allow external LSAs (type 5). To overcome this issue we are generating type 7 LSAs instead.

Designated Router and Backup DR:

Elect (**on boot) a DR**, everyone sends their updates to the **DR,** and then the **DR** updates everyone else with one BIG update (avoid traffic)

ID looks like an IP address. Highest wins.

Router 0# default information originate //shares the static routes (0.0.0.0!!!)

Passive Interfaces: Disable multicast updates, unicast works. The interface will **neither SENT** nor **RECEIVE** updates or hello packets (>> no NEIGHBOR relations!!)

#network 10.0.0.0 0.0.0.3 area 0 //area 0 = 0 backbone

OSPF Multi-Area

SPF - reduces traffic LSA - runs only on change

Routing table is smaller with multiple areas

- Backbone - Area 0 - High speed traffic
- Regular - end users - Area 1+

#Router ospf 1 //one OSPF process, different AREAS

#net xxxx area 0

#net xxxx area 1

#network xxxx 0.0.255.255 area 1

Wildcard Mask: the last two octets can match any number! = **RANGE OF HOSTS = FASTER to read**

OSPF Neighbor States:

(Darling) **Down** - no hello packets heard from neighbor

(I) Init - hello packet has been heard, but no 2-way communication

(Taste) Two-Way - 2-way communication established. **DR and BDR are elected. Hello Packets** carry a lists of the sender's known neighbors: | HELLO | R3 | R4 | << PACKET. The routers know see each other in the other's Hello packet!

(Some) ExStart - routers are preparing to exchange link-state info.

(Extremely) **Exchange** - exchanging of **Database Descriptors (DBDs)** - description of the router's **Topology Database.**Routers examine the neighbor's DBD to determine if it has info to share.

(Loud) **Loading** - routers are finally exchanging **LSAs**, containing information about all links connected. = Routers exchanging their topology tables

(Farts) **Full** - the routers are fully synchronized. The topology tables in the **AREA** are identical. **Full/(B)DR, /DROther** - **nor DR or BDR**

OSPF Network Types:

Broadcast Multi-Access - a topology where broadcast occurs.

Ethernet.... **OSPF** will elect **DRs and BDRs.** Traffic **TO DRs and BDRs: 224.0.0.6; traffic FROM DRs and BDRs: 224.0.0.5**

Neighbors must **not** be manually specified.

Point-to-Point - p2p - **NO DRs and BDRs** - all traffic is multicast 224.0.0.5 - Neighbors must **not** be manually specified.

Point-to-Multipoint - one interface can connect to multiple destinations - each connection is treated as **P2P. P2MP- Frame Relay**

Neighbors must **not** be manually specified.

Non-broadcast Multi-access Network (NBMA) - one interface <> multiple destination, NO broadcast whatsoever!

Frame Relay - **OSPF WILL elect DRs and BDRs** - Neighbors **MANUALLY** defined, thus all OSPF traffic is unicast, instead of multicast.

Internal Routers - all interfaces belong to the same **Area**

Backbone Routers - contains **at least** one interface in **Area 0**

Area Border Router (ABR) - belong to multiple areas, thus containing **multiple Topology DBs** for each.

Autonomous System Border Router (ASBR) - connects a separate **AS** or provides access to external networks (**Gateway?)**

> **Type 2 (E2) -** includes only the external cost **(default)**; **Type 1(E1)** - includes both external and internal cost (before and after the ASBR) = total metric. Type 1 > Type 2

Link-State Advertisements:

Link = router interface. From them and their states the **Topology DB** is created.

Router **LSA (Type 1) -** contains a list if all local links, the status and the cost. Generated by **ALL** routers and **flooded** to **ALL** within the **area.**

Network LSA (Type 2) - generated by **DR** - contains a list of ALL routers attached to the **DR.**

Network Summary (Type 3) - generated by all **Area Border Routers.** Contains a list of all destination networks within an area to allow **inter-area** communication.

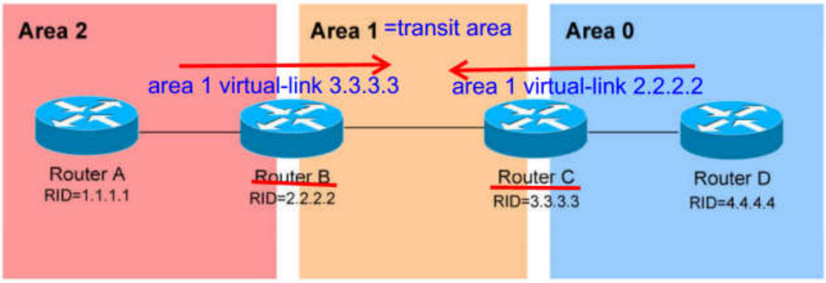
ASBR Summary (Type 4) - generated by **ABRs** and contains a route to **ANY ASBR** in the OSPF system (like a gateway)

External LSA (Type 5) - generated by **ASBR** and contains routes to destination networks **OUTSIDE** the **local AS.** Flooded to all areas of the OSPF system.

Virtual Links:

Area 2 must directly connect to **Area 0**, but doesn't have direct connection, so we use **Area 1** as **transit area.**

The two **Area Border Routers (ABRs)** 2 -> 1, and 1 -> 0 have to be configured = **TRANSIT AREA'S ABRS!!!**



It is also possible to have two **Area 0** (discontiguous) connected with a **virtual link.**

Area 0 <> Area 1 <> Area 0

```
RouterB# router-id 2.2.2.2                RouterC# router-id 3.3.3.3
RouterB# area 1 virtual-link 3.3.3.3      RouterC# area 1 virtual-link 2.2.2.2
```

===

13. EGP (Exterior Gateway Protocol) and BGP (Border Gateway Protocol).

Exterior protocols!!!

Router were called in the past **gateways. BGP** might also be referred as **EGP (Exterior Gateway Protocol).**

Exterior Gateway Protocol:

Obsolete!

It was designed with a **concrete Internet Topology** in mind **- hierarchical tree -** with a **CORE** as the root.

IT CANNOT HANDLE ARBITRARY TOPOLOGIES LIKE BGP CAN ! Therefore it can't guarantee the absence of **routing loops.**

Responsible for exchange of network reachability information between neighboring routers, which MAY or MAY **NOT** be in different AS.

Each EGP router maintains a **DB** of information what networks it can reach and **HOW TO.**

Sends information **REGULARLY** to each router to which it's directly connected. Routers receive these updates and update their routing tables, and then use this info to update other routers.

Exchanging Routing Information:

- **Neighbor Acquisition:** each router sends **Neighbor Acquisition Request**. A neighbor hearing this responds with **Neighbor Acquisition Confirm** or with **Refuse.** For an EGP connection to establish, each must first acquire the other with **Confirm message.**
- **Neighbor Reachability: regularly** each router checks the neighbors are reachable by sending **EGP Hello messages**. The neighbors reply with an **I HEARD YOU (IHU) message**. (Like **BGP Keepalive** message).
- **Network Reachability Update:** a router sends **Poll messages** regularly to each of its neighbors. They respond with an **Update message,** with details about the networks it can reach. This info is used to update the routing info on the device that sends the **Poll.**

Breaking Neighbor Relations:

A connection is terminated by sending a **Neighbor De-Acquisition** (**Cease Message).** The neighbor responds with a **Cease-ack(nowledge) message.**

Error Reporting:

- When a received EGP message has a problem, the router responds with an **Error message.**

Border Gateway Protocol(overview):

The routing protocol of choice on the Internet, since the Internet is just interconnected Autonomous Systems.

The slowest routing protocol in the world! >> new domain ? Takes days to come online! (flapping routes)

It is designed to work on the edge of your network, passing routing information about the structure of your network beyond the gateway.

This information can then be sent on to other BGP routers, informing them which networks are found behind the BGP router.

BGP routers announce router that they have learned and also **re-transmit** router learned from the **IGPs** on their networks.

BGP also exchanges network reachability and availability information for the **AS.** This allows the construction of **topology graphs** on both sides of the **BGP link. Topology graphs** also help to identify **loops** and other **issues.**

Version **4** is the current. Two **BGP** systems try to communicate at version **4**, and if it's not supported by both sides, they negotiate down until they find a suitable version.

Administrative distance: WEIGHT.

AD can be modified - 0 - 65535. **Cisco default 32768. HIGHER = PREFFERED !**

How does BGP choose routes ? (Paths):

Adds the AS number from which the router has been learned:

56-910 means that the route was learned from AS **56**, which had learned it from AS **910**.

Vs

34-78-910 - is longer and **LOOSES** to **56-910.**

As far as the local AS does not show up in the PATH there are no loops.

BGP support CIDR > router summarization (supernetting) > limiting the entries in the routing table.

Autonomous System Number (ASN) 1 - 65535. **AS -** connected group of IP prefixes which has a SINGLE and CLEARLY Defined routing policy

BGP uses **TCP** for reliable transfer, **port 179**

BGP store more complete information (than just the **NEXT HOP**) about the path (sequence of ASs), special **path attributes** describe the characteristics of the paths.

Each **AS** assigns one or more routers to use the protocol, then they communicate with each other.

BGP Policies: like if an AS is willing to carry traffic from other ASes or not.

Flexibility: the protocol can connect ANY internetwork of ASes using any topology, they only requirement is that each AS have at least one router that is able to run BGP and it can connect to eat least one other router running BGP.

BGP Speaker: designated routers within the AS to run BGP.

BGP Traffic Flow and Types:

- **Local Traffic -** either originated in the AS, or is intended to be delivered in the AS
- **Transit Traffic -** originated outside the AS and is to be delivered outside the AS

Autonomous System TYPES:

- **Stub AS - AS** connected to only one other AS (dead end street).
- **Multihomed AS - AS** connected to two or more ASes

System Routing Policies:

- **No Transit Policy -** no transit traffic
- **Restricted AS Transit Policy -** transit traffic only from certain ASes. It tells the ASes it will handle their traffic, but does not say this to the others.
- **Criteria-Based Transit Policy -** only during certain times, or when it has capacity to spare

Messages:

- OPEN - contact neighbors and establish sessions
- UPDATE - exchange information about reachable networks (partial information)
- KEEPALIVE - maintain sessions
- NOTIFICATION - inform of error

Databases:

- **Neighbor DB (BGP Specific) -** all configure **BGP neighbors** // show ip bgp summary
- **BGP DB (BGP Specific)** - list of networks known by BGP + paths + attributes // show ip bgp
- **Routing Table - (Universal) -** paths to each network used by the router, and the next hop // show ip route

Internal and External BGP:

- **iBGP - relationship between routers in the same AS**
- **eBGP - between routers in different AS** (two edge routers)

(BGP treats updates from internals different from external peers)

==

14. Integrated IS-IS (Intermediate System to Intermediate System).

Intermediate System = router (OSI term)

Much similar to OSPF (also **Link-State**). It is mainly used by ISPs due to its scalability.

Support IPv4 and IPv6

IS-IS has the Link-State characteristics:

- Hierarchical design using **Areas**
- Form **neighbor** relations with adjacent routers using IS-IS
- Advertises the status of the directly connected **links** as **Link-State Packets (LSPs)**.
- Updates are send **ONLY** when there's a change on one of the links and including **ONLY** the change.
- Dijkstra Shortest Path First algo.
- **Classless** > supports VLSM
- Designed to route the ISO address space >> NOT Properiarity - supports IPX, Apple Talk…
- **AD = 115**
- **Cost is arbitrary** - **delay, expense, and error.**

Tables:

- **Neighbor -** list of all neighbors
- **Topology -** list of all **possible** routes to all known networks **within** an **area**
- **Routing -** contains only the **best** route for each known network

Three Sub-Protocols:

- **CLNP (Connectionless Network Protocol)** - serves Layer 3 protocols for IS-IS (developed by ISO) **NOT VERY USED!**
- **ES-IS (End System-to-Intermediate System)** - route between **HOSTS and ROUTERS.**
- **IS-IS (Intermediate System-to-Intermediate System)** - route between **ROUTERS**

== Connectionless Network Service (CLNS)

CLNP Address: hex and varying length - 64 to 160 bits - 3 sections: area (var) + ID (8 to 64, usually 48 bits) + Selector (8bits)

IS-IS Packet Types:

- **ES (End System) -** end host
- **IS (Intermediate System) -** L3 router

Packets:

- **Hello** - for neighbor discovery - **Three types** - **IIH (IS-IS Hello); ESH (ES Hello); ISH (IS Hello)**
- **LSP** - **Link State Packet** - share topology info between routers - separate between **Level 1 and Level 2**
- **CSNP** - Complete Sequence Number PDU - update containing the full **link-state DB.** Refreshed every **15 mins.**
- **PSNP** - Partial Sequence Number PDU - both **request and acknowledge** a link-state update.

IS-IS Neighbors:

- Adjacencies are formed after sending **HELLO packets (IIH) every 10 seconds** regardless of media**.** After that routers can share info.
- **IS-IS** neighbors require no IP connectivity! Adjacencies are formed across **CLNP (Connectionless Network Protocol)**

Three types of IIH packets: one for P2P and two for broadcast(LAN) (L1 and L2 broadcast Hellos)

Passive Interfaces:

Like **OSPF** it will **NOT** form neighbor relationships through them, nor updates pass through them!!

UNLIKE OSPF, the command will still inject that interface's network into the routing table (STUB NETWORKS)

Metric:

Arbitrary cost! Delay, expense, and error are not supported by cisco. **Default metric = 10.**

#interface e0/0

#isis metric 30

===

15. Advanced IP Routing Issues: Network Address Translation (NAT). Introduction to IP Multicast Routing, Protocol Independent Multicast (PIM), Large-Scale IP Multicast Routing.

A **public** address can be routed on the Internet. Thus, hosts that must be Internet-accessible must be configured with (or *reachable* by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).

A **private** address is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses.

NAT (Network Address Translation) - it is possible to translate between private and public addresses. It allows (one or more!) private address to be **stamped** with a public address, allowing it to communicate across the Internet.
NAT also hides the specific inside addresses and the structure of the network.
Also supports public-to-public and private-to-private translations.

Introduction to IP Multicasting:

A multicast address is designed to enable the delivery of datagrams to a set of hosts - members of a multicast group in various subnets.

Multicast is NOT connection-oriented - the "best-effort" as a standard IP Datagram (UDP?) is used >> It's not guaranteed that a datagram will reach all members of the group, or arrive in the same order of transmission.

Class D Address: 224.0.0.0 - 239.255.255.255 - 1110.x.x.x

A member is free to join or leave any group at any time. There is no restriction on the physical location or the members in a multicast group. A host may be a member of more than one multicast group. Anyone can send messages to a multicast group.

VS Unicast:

- Sender must generate packet for each receiver and know all addresses
- Routers must process packets for each receiver separately

- Bandwidth is proportional to the number of receivers

Multicast: sends the information one time and routers replicate and distribute to the receivers (one packet per interface)

Sends UDP multicast traffic with 'group' internet address.

Layer 3: IPv4/v6 addresses

Layer 2: MAC addresses

Control Plane Protocols:

IGMP & PIM(Protocol Independent Multicast)

(S,G) - source + group address (1.2.3.4, 224.1.1.1)

Traffic is always sent **TO**, never **FROM** a group

Host Membership Report - request to join a group

Host Membership Query - anyone listening to this group ? Dead timer

PIM - Independent, because does not advertise its topology

Multicast is routed through a network which also routes unicast with a type of **IGP**, therefore there should be no loops. **PIM** doesn't need to exchange routing info.

- **Reverse Path Forwarding (RPF)** - **INBOUND CHECK -** checks for **temporary** problems in the network - **every incoming** multicast packet it checks BACK if it was received on the correct interface. Look at SOURCE address, Lookup how I would route BACK to that address. **IF In**bound interface = **OUT**bound interface = **PASS!** Otherwise the packet is **dropped**.

ONE PATH FROM SENDER TO RECEIVER!

- **Multicast Routing Table (MRIG/MFIB)** - **OUTBOUND** - Split Horizon like behavior - assumes that the incoming packets passed the RPF are loop free. Routing is based on the **PIM JOIN** or **IGMP REPORT**(**JOIN**) messages (I want to receive multicast). Incoming traffic is being forwarded to the **Outgoing Interface List (OIL).** A link cannot be INCOMING and OUTGOING at the same time
- If **RPF passes** , packets flow from incoming interface to all interfaces in **OIL.**

Group Membership Protocol:

Large-Scale IP Multicast Routing:

Primary consideration is limiting the scope of the domain:

- **TTL Scoping - LACKS FLEXIBILITY -** the TTL of the packets is altered, so that each packet could travel only a certain distance.

Can be configured per-interface basis for multicast packets: #ip multicast ttl-threshold 5. **Only** packets with threshold **MORE** than 5 are fowared through it! Other will be dropped.

TTL 0 = 0 same host; 1 = subnet; 15 = same site; 63 = same region; 127 = worldwide; 191 = worldwide limited bandwidth; 255 = unrestricted

- **Administrative Scoping - MORE FLEXIBLE -** the multicast address range (224 - 239.255.255.255) is partitioned to certain scopes.

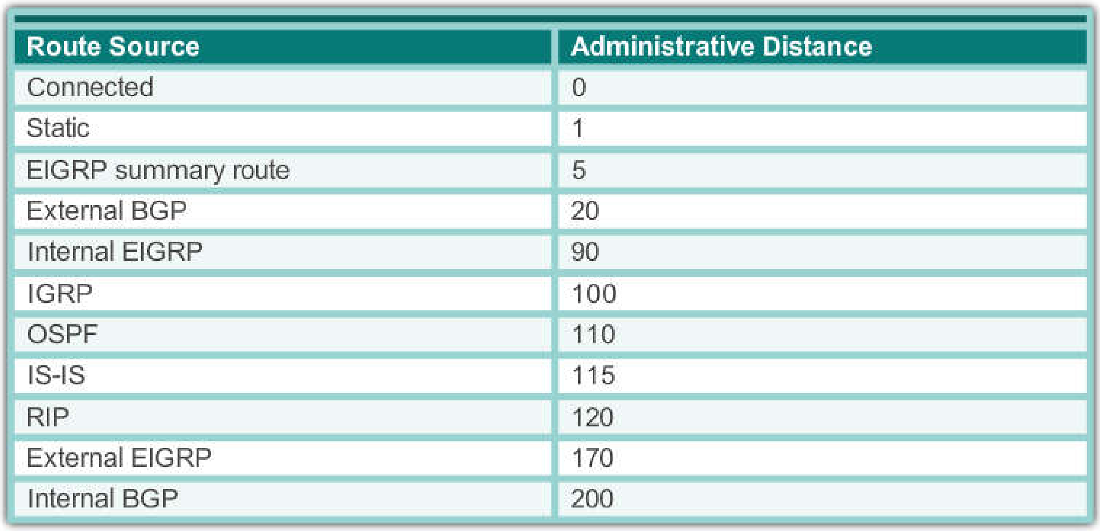
OSPF and EIGRP 224.0.0.5 .6 and .10 are considered **local-link** are not forwarded by routers.

224.0.0.0/24 - link-local scope, 224.0.1.0-238.255.255.255 - global, 239.192.0.0/14 - organization-local scope

==

==

MISCELANOUS:



Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

#show ip interface brief

A router connects multiple networks, which means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.

LANs are commonly Ethernet networks that contain devices, such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area. For example, a WAN connection is commonly used to connect a LAN to the Internet service provider (ISP) network.

The primary functions of a router are to:

- Determine the best path to send packets -routing table
- Forward packets toward their destination - destination ip address > table > interface

- Process switching solves a problem by doing math long hand, even if it is the identical problem.
- Fast switching solves a problem by doing math long hand one time and remembering the answer for subsequent identical problems.
- Cisco Express Forwarding solves every possible problem ahead of time in a spreadsheet.

SERIAL = P2P = NO SOURCE REQUIRED !!
SERIAL DESTINATION = BROADCAST, because no MAC addresses

The following lists some dynamic protocols and the metrics they use:

- **Routing Information Protocol (RIP)** - Hop count
- **Open Shortest Path First (OSPF)** - Cisco's cost based on cumulative bandwidth from source to destination
- **Enhanced Interior Gateway Routing Protocol (EIGRP)** - Bandwidth, delay (,load, reliability)

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing

Network discovery is the ability of a routing protocol to share information about the networks that it knows about with other routers that are also using the same routing protocol. Routers have converged after they have finished exchanging and updating their routing tables, they also determine a new best path if the initial path becomes unusable (or if the topology changes) without involving the network administrator.
D = EIGRP; * = possible default route;
EX = external, forwarded by EIGRP
Routers make their primary forwarding decision at Layer 3, the Network layer. However, router interfaces participate in Layers 1, 2, and 3. Layer 3 IP packets are encapsulated into a Layer 2 data link frame and encoded into bits at Layer 1. Router interfaces participate in Layer 2 processes associated with their encapsulation. For example, an Ethernet interface on a router participates in the ARP process like other hosts on that LAN.

CHAPTER 6 STATIC ROUTING

Static routes are very common and do not require the same amount of processing and **overhead** as dynamic routing protocols.
Static routes are not advertised over the network >> SECURITY!
Static route **AD = 1**, always preferred over dynamically learned.
Static route with EXIT INTERFACE **AD = 0**
Static routes remain in the routing table as long as it's INTERFACE stays UP > # ip route IP MASK NEXT-HOP ***permanent***
Static routes can be used to discard traffic to a **virtual null interface** > # ip route 10.0.0.0 255.0.0.0 **null0**
To reduce the number of routing table entries, multiple static routes can be summarized into a single static route if:
The destination networks are contiguous and can be summarized into a single network address.
The multiple static routes all use the same exit interface or next-hop IP address.

Another type of static route is a floating static route. Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure. The floating static route is only used when the primary route is not available.

To accomplish this, the floating static route is configured with a higher administrative distance than the primary route. Recall that the administrative distance represents the trustworthiness of a route.

Global config:

```
Router(config)# ip routenetwork-address subnet-mask {ip-address | interface-type interface-number [ ip-address ]} [ distance ] [ name name ] [permanent ] [ tag tag ]
```

The subnet mask can be modified to summarize a group of networks.

Static routes have : Next hop addr. or exit interface

Resolve: 192.168.2.0/24 via 172.16.2.2

Resolve: 172.16.2.2 from the routing table (Serial0/0/0) (RECURSIVE LOOKUP)

Note: For point-to-point interfaces, you can use static routes that point to the exit interface or to the next-hop address. For multipoint/broadcast interfaces, it is more suitable to use static routes that point to a next-hop address.

Fully specified static route = Next Hop + Exit Interface!!!

Default static routes are commonly used when connecting:

An edge router to a service provider network

A stub router (a router with only one upstream neighbor router)

S* 0.0.0.0/0 via …

S = static; * = candidate; /0 none of the bits must match

The **ipv6 unicast-routing** global configuration command must be configured to enable the router to forward IPv6 packets.

CLASSFUL ADDRESSING

As shown in Figure 1, class A networks used the first octet to identify the network portion of the address. This is translated to a 255.0.0.0 classful subnet mask. Because only 7 bits were left in the first octet (remember, the first bit is always 0), this made 2 to the 7th power, or 128 networks. The actual number is 126 networks, because there are two reserved class A addresses (i.e., 0.0.0.0/8 and 127.0.0.0/8). With 24 bits in the host portion, each class A address had the potential for over 16 million individual host addresses.

As shown in Figure 2, class B networks used the first two octets to identify the network portion of the network address. With the first two bits already established as 1 and 0, 14 bits remained in the first two octets for assigning networks, which resulted in 16,384 class B network addresses. Because each class B network address contained 16 bits in the host portion, it controlled 65,534 addresses. (Recall that two addresses were reserved for the network and broadcast addresses.)

As shown in Figure 3, class C networks used the first three octets to identify the network portion of the network address. With the first three bits established as 1 and 1 and 0, 21 bits remained for assigning networks for over 2 million class C networks. But, each class C network only had 8 bits in the host portion, or 254 possible host addresses.

Summary and Floating Static routes

Another type of static route is a floating static route. Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure. The floating static route is only used when the primary route is not available.

To accomplish this, the floating static route is configured with a higher administrative distance than the primary route. Recall that the administrative distance represents the trustworthiness of a route.