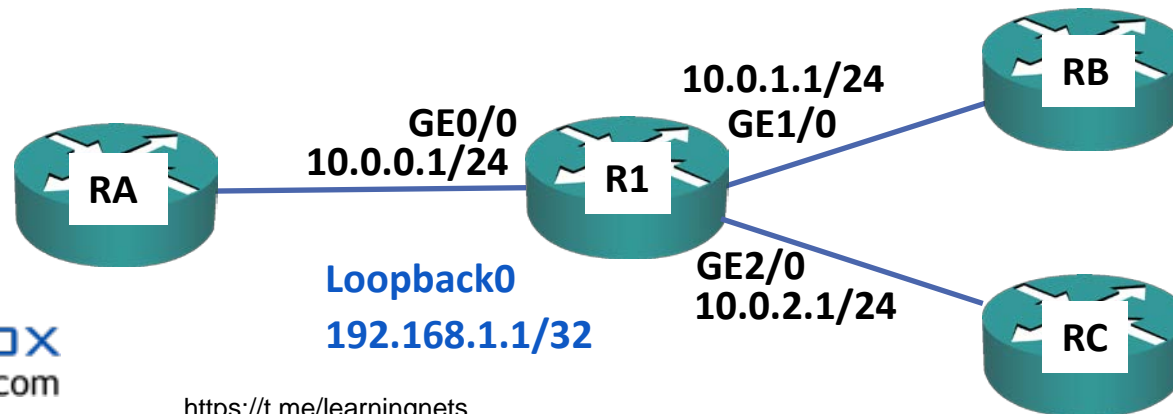


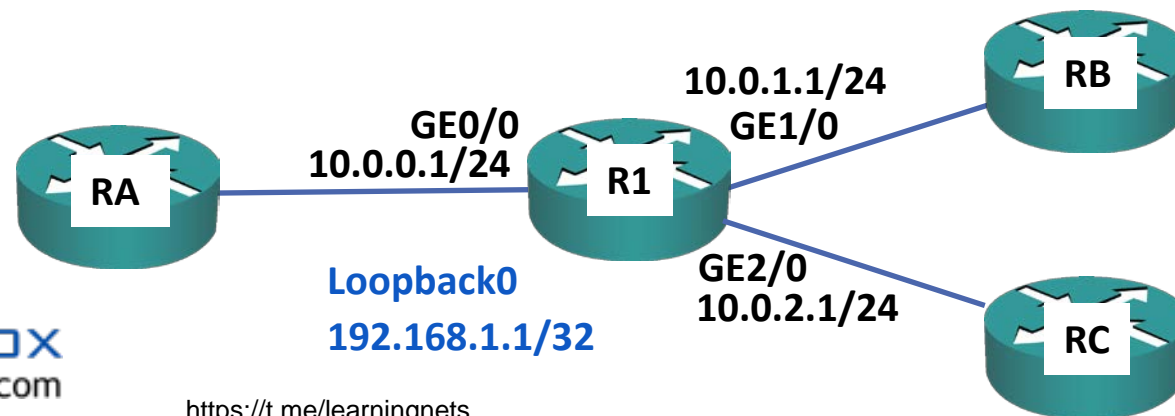
# Passive Interfaces

- Passive interfaces allow you to include an IP subnet in the routing protocol without sending updates out of the interface
- If GigabitEthernet2/0 is configured as a passive interface, RA and RB will learn routes to 10.0.2.0, but internal network information will not be sent to RC
- If the routing protocol was not enabled on GigabitEthernet2/0 at all, RA and RB would not learn routes to 10.0.2.0



# Passive Interfaces

- It is best practice to configure loopback interfaces as passive interfaces
- It is impossible to form an adjacency on a loopback interface because they are not physical interfaces
- Making the loopback passive means that it will be advertised by the routing protocol but it will not waste resources sending out and listening for hello packets



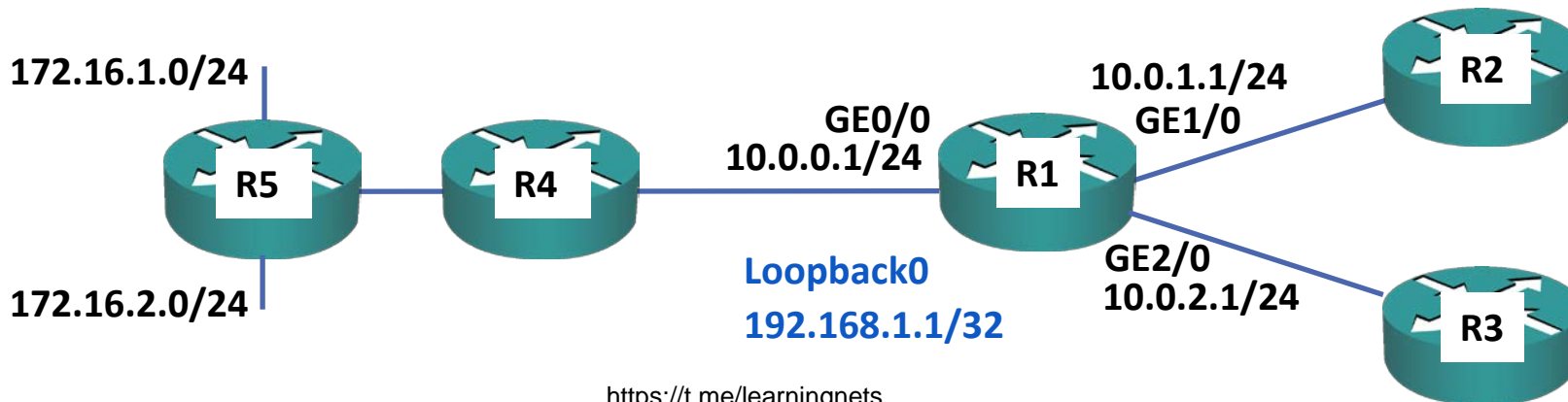
# Passive Interface Use Cases



- Passive interfaces are used on:
  - Loopback interfaces
  - Physical interfaces where the device on the other side belongs to another organisation. We do not want to send routing information out but we do want our internal devices to know about the link

# Route Filtering

- Route filtering allows certain specified routes to not be advertised outbound, or accepted inbound
- For example below, R1 could be configured to not advertise the 172.16.2.0/24 network, or R2 could be configured to not accept it
- All other routes would be learned by all routers
- Note that R1 is not directly connected to the 172.16.2.0/24 network. Filtering does not have to take place at the source



# Route Filtering



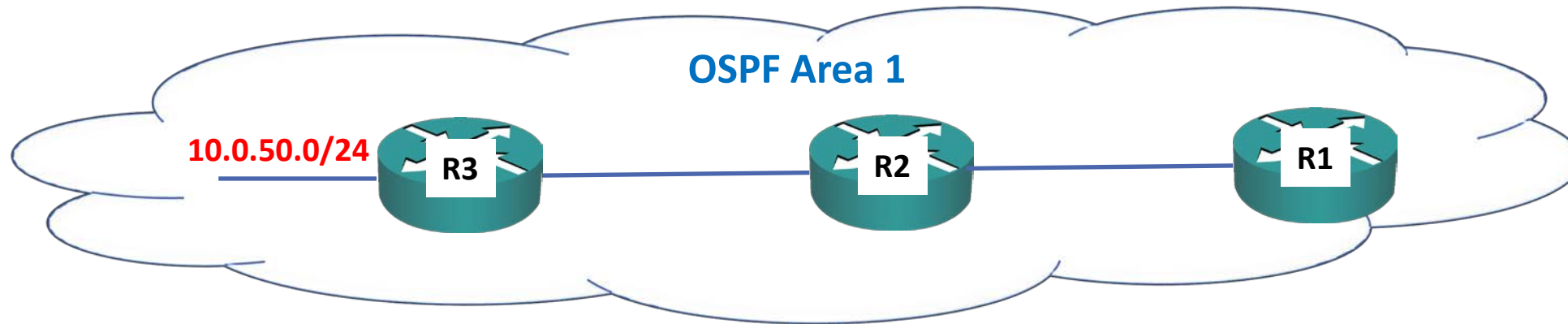
- In all routing protocols on Cisco routers, route filters can be applied:
  - On router interfaces
  - When redistributing routes between routing protocols
- Some routing protocol specific filtering tools are also available, such as OSPF Area Filtering, and BGP AS Path Filtering

# Outbound Filtering – Link State Protocols

- All routers in an OSPF area must have the same LSDB
- Routes cannot be filtered **outbound** at the interface level because of this
- Outbound filtering is supported between areas and when redistributing into another routing protocol
- OSPF routers can filter **incoming** routes at the interface level. The routes will still enter their LSDB but they will be filtered out of the routing table
- IS-IS is also a link state routing protocol so has the same rules

# Distance Vector vs Link State Route Filtering

- With link state routing protocols, every router in an area must share the same complete copy of the link state database.



- All routers in Area 1 must have 10.0.50.0/24 in their LSDB.
- Inbound interface route filters can be applied on both R2 and R3 to prevent the route from being installed into their routing tables.
- The route filter applies to only that individual router.

# Area Filtering – Link State Protocols



- OSPF routers maintain separate Link State Databases for separate areas
- Route filters can also be applied at the Area level in Link State routing protocols (as well as the interface level and when redistributing)
- Area level filters control which routes exit or enter an area

# Outbound Filtering – Distance Vector Protocols

- Routes can be filtered both inbound and outbound at the interface level in distance vector routing protocols (RIP, EIGRP) and the path vector routing protocol BGP
- Filtered routes do not appear in the routing protocol database (eg EIGRP topology table) or the routing table

# Distance Vector vs Link State Route Filtering

- R2 will not advertise the route to 10.0.50.0/24 to R1 because it has already been filtered out.



# Route Filtering Use Cases - IGP



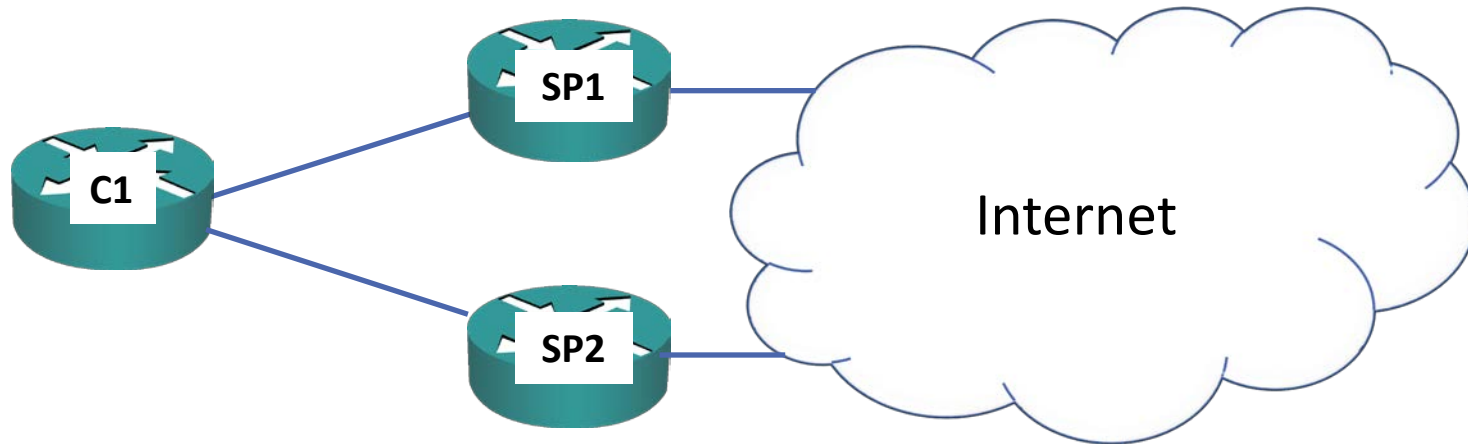
- Inside an organization, all the company's routers are usually running the same IGP and know routes to all internal networks
- Access Control Lists are commonly used to secure traffic flows within the organization
- Route Filters can be used to stop IGP routers within an organisation from having routes to internal networks
- This can be useful when, for example:
  - Using an IGP while connecting to a partner company on an Extranet - outbound to ensure only allowed networks are advertised, and inbound to prevent invalid routes being received
  - Redistributing between routing protocols

# Route Filtering Use Cases - BGP



- Route Filtering is used very commonly in BGP, for example:
  - To limit size of routing table to conserve router memory
  - To ensure only valid routes are received from a neighbor (prevent address hijacking)
  - To prevent transit of Internet traffic through a multi-homed organisation

# Multi-Homed Customer with BGP



# Route Filter Operation



- **Routes to be filtered** can be specified with an Access Control List or Prefix List
- ACLs and Prefix Lists can optionally be nested inside a Route Map
- The filter is **applied** with a Distribute List
- (Prefix Lists can be applied directly to neighbors in BGP)