رواد مصر الرقمية

Skills Dynamix

Configure and Troubleshoot OSPF and EIGRP

رواد مصر الرقمية

Skills Dynamix

Today's Agenda

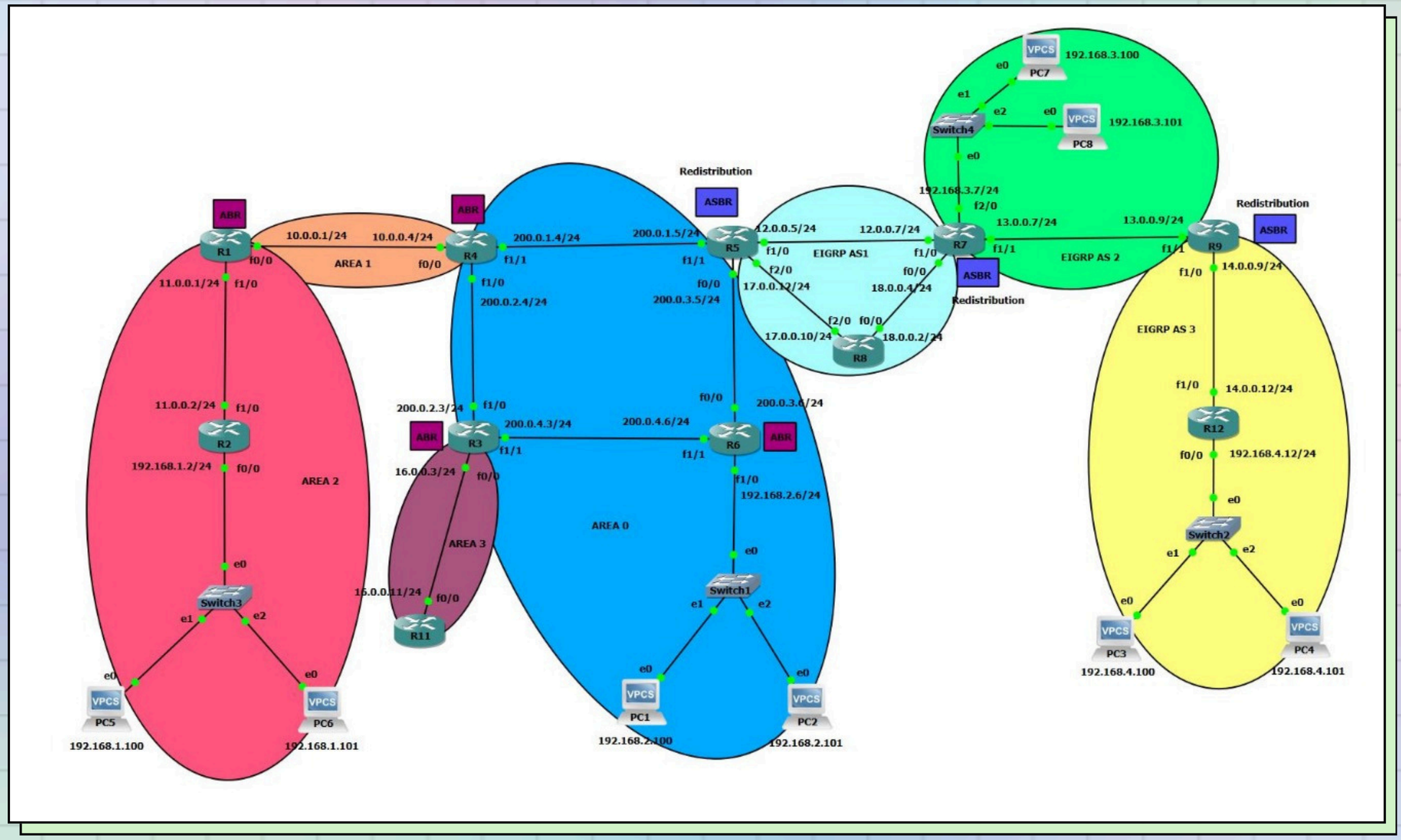
1. Introduction to the Project
2. Routing
3. OSPF
4. EIGRP
5. Troubleshooting
6. Security

Project Idea

This project focuses on designing and implementing two distinct enterprise networks using Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)

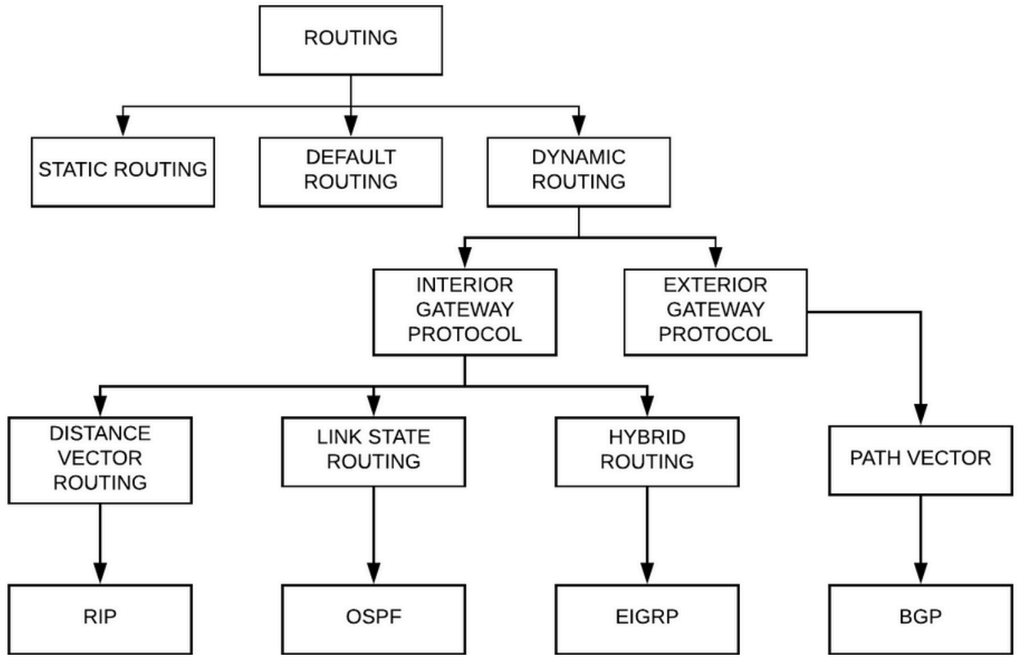
OSPF, a link-state protocol, and EIGRP, a distance-vector protocol, are configured within separate domains to meet specific network requirements. The core objective is to enable communication between these two protocols using route redistribution, ensuring efficient and seamless data exchange across both networks.

Project View



Routing

Routing is the process of selecting the best path for data to travel across networks. When data, in the form of packets, moves from one device to another, routing ensures it takes the most efficient and reliable path to reach its destination. Routers, which are specialized devices or software functions, play a key role in directing this traffic.



OSPF

Open Shortest Path First (OSPF) is a dynamic link-state routing protocol used within an autonomous system (AS) to determine the most efficient route for data packets across a network. It operates using the Shortest Path First (SPF) algorithm, also known as Dijkstra's algorithm, to calculate the best paths based on various network metrics, such as bandwidth and delay.

Key Features of OSPF

1. Hierarchical Design
2. Router ID
3. Link-State Advertisements
4. Adjacency Formation
5. Fast Convergence
6. Cost Metric

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol developed by Cisco. It combines the features of both distance-vector and link-state protocols, making it highly efficient for both small and large enterprise networks. EIGRP is known for its fast convergence, efficient use of bandwidth, and flexibility in handling complex network topologies.

Key Features of EIGRP

1. Dual Algorithm (DUAL)
2. Metrics using three things
3. Partial Updates
4. Neighbor Relationships
5. Route Summarization
6. Fast Convergence

OSPF	EIGRP
builds a complete map of the network, ensuring each router has full visibility of the network's topology	calculates the best path to a destination using information from directly connected neighbors, but it also includes link-state features
Uses Dijkstra's Shortest Path First (SPF) algorithm to calculate the shortest path based on link cost.	Uses Diffusing Update Algorithm (DUAL) to calculate the best path based on composite metrics, and it can quickly converge by using backup paths.
Metric is based on link cost, which is typically influenced by bandwidth. The lower the cost, the better the route.	Uses a composite metric that considers bandwidth, delay, load, reliability, and MTU (by default, only bandwidth and delay are used).
Has a full view of the network due to the link-state nature and creates a network-wide map (topology table).	Only knows the best path from itself to a destination and does not have full network topology visibility, using a neighbor table for routing decisions.
Supports hierarchy with areas to optimize large networks, with a mandatory backbone area (Area 0) that connects other areas.	Does not require hierarchical design, though manual route summarization is supported.

OSPF	EIGRP
Relies on periodic LSA updates and recalculates paths, making it slower to converge in some cases.	Converges faster due to DUAL and uses feasible successors (backup routes) to minimize downtime during failures.
Sends full updates at specific intervals which can be bandwidth-intensive but ensures an up-to-date map of the network.	Sends partial updates only when there is a change in the network, and only for the affected routes, making it more bandwidth-efficient.
More scalable due to its area-based design, especially in large, complex networks.	Scalable, but more efficient for Cisco-specific environments and less so in multi-vendor environments.
Vendor-neutral, supported by almost all network vendors, making it ideal for heterogeneous networks.	Cisco proprietary, though it has been made an open standard in recent years, but is still primarily used in Cisco-based networks.
Supports clear-text and MD5 authentication to ensure secure routing updates between neighbors.	supports MD5 authentication to ensure the integrity of routing information.

Security

ACL

Access Control List is a set of rules applied to network devices (such as routers and firewalls) to control the flow of traffic. ACLs define which packets are allowed or denied based on specific criteria, such as IP addresses, protocols, or ports.

SSH

Secure Shell is used to establish a secure, encrypted connection for remote management and configuration. Unlike older protocols such as Telnet, which sends data in plaintext, SSH ensures that the connection is secure, protecting the router from unauthorized access or eavesdropping.

رواد مصر الرقمية

Skills Dynamix

Thank you!

Have a great day ahead.