

Subnetting Scheme:

LAN

Provided IP: 10.0.0.0/11

Country	Network Address	Subnet Mask	First Usable	Last Usable	Broadcast	Hosts
Qatar	10.0.0.0	255.255.252.0	10.0.0.1	10.0.3.254	10.0.3.255	789
Riyadh, Saudi	10.0.4.0	255.255.254.0	10.0.4.1	10.0.5.254	10.0.5.255	300
Oman	10.0.6.0	255.255.254.0	10.0.6.1	10.0.7.254	10.0.7.255	330
Dubai, UAE	10.0.8.0	255.255.255.0	10.0.8.1	10.0.8.254	10.0.8.255	150
Damam, Saudi	10.0.9.0	255.255.255.0	10.0.9.1	10.0.9.254	10.0.9.255	200
Kuwait	10.0.10.0	255.255.255.0	10.0.10.1	10.0.10.254	10.0.10.255	170
Ajman, UAE	10.0.11.0	255.255.255.128	10.0.11.1	10.0.11.126	10.0.11.127	90
Bahrain	10.0.11.128	255.255.255.224	10.0.11.129	10.0.11.158	10.0.11.159	20
Cloud Server	10.0.11.160	255.255.255.240	10.0.11.161	10.0.11.174	10.0.11.175	5
Unused: 10.0.11.176 – 10.31.255.255						

WAN

Provided IP: 211.168.0.0/22

Country	Network Address	Subnet Mask	First Usable	Last Usable	Broadcast
Qatar – Gulf	211.168.0.0	255.255.255.252	211.168.0.1	211.168.0.2	211.168.0.3
Doha – Cloud Link 1	211.168.0.4	255.255.255.252	211.168.0.5	211.168.0.6	211.168.0.7
Doha – Cloud Link 2	211.168.0.8	255.255.255.252	211.168.0.9	211.168.0.10	211.168.0.11
Saudi – Gulf	211.168.0.12	255.255.255.252	211.168.0.13	211.168.0.14	211.168.0.15
Saudi – Riyadh	211.168.0.16	255.255.255.252	211.168.0.17	211.168.0.18	211.168.0.19
Saudi – Damam	211.168.0.20	255.255.255.252	211.168.0.21	211.168.0.22	211.168.0.23
UAE – Gulf	211.168.0.24	255.255.255.252	211.168.0.25	211.168.0.26	211.168.0.27
UAE – Dubai	211.168.0.28	255.255.255.252	211.168.0.29	211.168.0.30	211.168.0.31
UAE – Ajman	211.168.0.32	255.255.255.252	211.168.0.33	211.168.0.34	211.168.0.35
Oman – Gulf	211.168.0.36	255.255.255.252	211.168.0.37	211.168.0.38	211.168.0.39
Kuwait – Gulf	211.168.0.40	255.255.255.252	211.168.0.41	211.168.0.42	211.168.0.43
Bahrain – Gulf	211.168.0.44	255.255.255.252	211.168.0.45	211.168.0.46	211.168.0.47
<u>Unused:</u> 211.168.0.48 – 211.168.3.254					

IPV6: 2003:0DB8:C21A::/48

Country	Network Address	Hosts
Kuwait	2003:0DB8:C21A::/64	170
Bahrain	2003:0DB8:C21B::/64	20
Bahrain – Gulf (WAN)	2003:0DB8:C21C::0/64	-
Kuwait – Gulf (WAN)	2003:0DB8:C21D::0/64	-

IP Assigning and GSP Buildings

In this network configuration, all GSP buildings are set up with Ipv4 addressing. Meanwhile, the branches in Kuwait and Bahrain are configured with dual-stack capabilities, supporting both Ipv4 and Ipv6. Ipv4 is designated for external communication with other branches, such as Qatar and the UAE. On the other hand, Ipv6 is specifically employed for internal communication between the Kuwait and Bahrain branches, facilitating the exchange and forwarding of traffic within these locations.

The routers are configured to route Ipv4 traffic between GSP buildings and Kuwait/Bahrain branches, while Ipv6 routing is enabled for communication within the Kuwait and Bahrain branches. The switches are configured to enable Ipv6 for internal communication, and Ipv4 addressing is set up on interfaces for external communication from GSP buildings. This approach ensures a seamless and efficient network operation with the coexistence of Ipv4 and Ipv6 protocols.

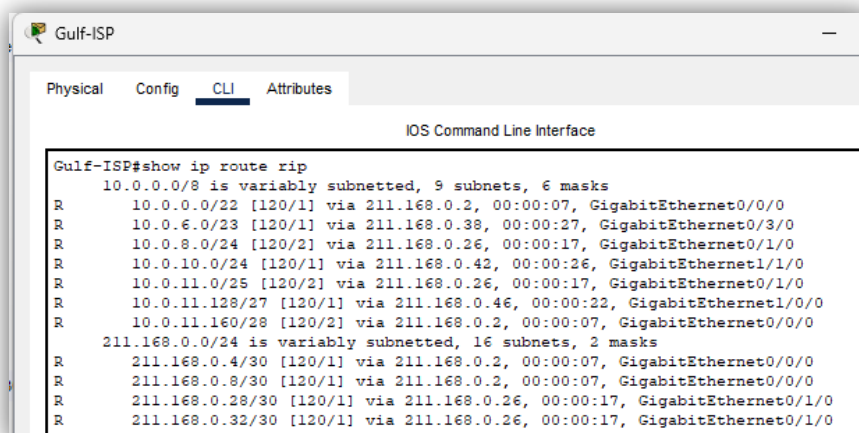
RIP v2 and RIPng

Routing Information Protocol Version 2 (RIP v2) serves as a distance-vector routing protocol specifically designed for Ipv4 networks. RIP v2 supports subnetting, enabling more efficient IP address allocation and the routing of subnets with variable lengths through Variable Length Subnet Masking (VLSM). The protocol employs a hop count metric to determine the optimal route. Furthermore, RIP v2 includes authentication features to ensure the security of routing information, a critical aspect in the context of larger networks.

Routing Information Protocol Next Generation (RIPng) is tailored for Ipv6 networks, providing similar simplicity and ease of configuration. While maintaining the hop count metric for route selection, RIPng uses Ipv6 addressing in its updates. RIPng minimizes unnecessary network traffic. Like RIP v2, RIPng supports authentication, enhancing security for routing updates in Ipv6 environments. Both RIP v2 for Ipv4 and RIPng for Ipv6 are recognized for their user-friendly nature, making them particularly suitable for smaller networks where advanced features are not the primary focus.

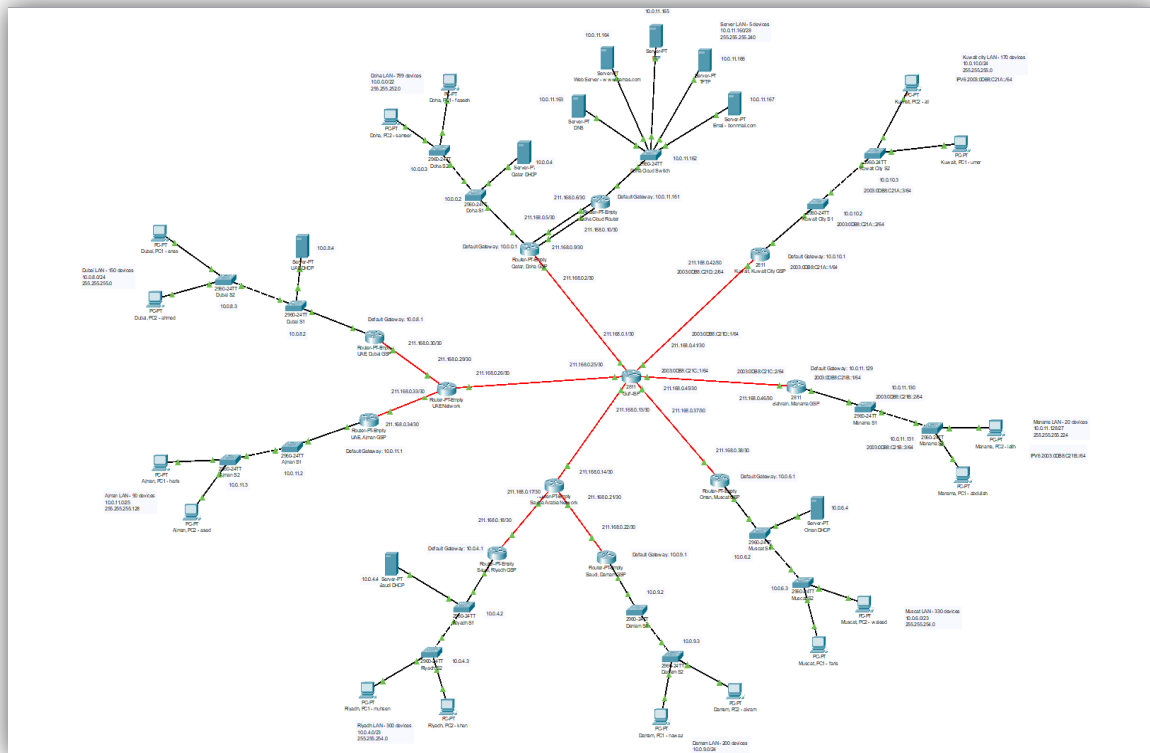
In our scenario here, we implemented RIP v2 for all GSP buildings and their routings. This included all routers within all networks and the main Gulf router as well. On the other hand, RIPng was implemented only in Kuwait, Bahrain and the Gulf Router ports that connect to these 2 networks. With such a scenario, we had flawless pinging and connections of pcs across multiple WANS without any issues.

Gulf ISP Core Router – Routing Information



```
Gulf-ISP#show ip route rip
10.0.0.0/8 is variably subnetted, 9 subnets, 6 masks
R    10.0.0.0/22 [120/1] via 211.168.0.2, 00:00:07, GigabitEthernet0/0/0
R    10.0.6.0/23 [120/1] via 211.168.0.38, 00:00:27, GigabitEthernet0/3/0
R    10.0.8.0/24 [120/2] via 211.168.0.26, 00:00:17, GigabitEthernet0/1/0
R    10.0.10.0/24 [120/1] via 211.168.0.42, 00:00:26, GigabitEthernet1/1/0
R    10.0.11.0/25 [120/2] via 211.168.0.26, 00:00:17, GigabitEthernet0/1/0
R    10.0.11.128/27 [120/1] via 211.168.0.46, 00:00:22, GigabitEthernet1/0/0
R    10.0.11.160/28 [120/2] via 211.168.0.2, 00:00:07, GigabitEthernet0/0/0
211.168.0.0/24 is variably subnetted, 16 subnets, 2 masks
R    211.168.0.4/30 [120/1] via 211.168.0.2, 00:00:07, GigabitEthernet0/0/0
R    211.168.0.8/30 [120/1] via 211.168.0.2, 00:00:07, GigabitEthernet0/0/0
R    211.168.0.28/30 [120/1] via 211.168.0.26, 00:00:17, GigabitEthernet0/1/0
R    211.168.0.32/30 [120/1] via 211.168.0.26, 00:00:17, GigabitEthernet0/1/0
```

Network Diagram



In our network configuration, we employed a star topology where multiple networks are connected to a central router known as the Gulf ISP Router. This structured layout facilitates efficient management, allowing each device in the network to communicate directly with the central router. This centralized design streamlines network tasks, providing a clear overview of the entire system.

In our design, we chose to assign a router for each city which connects to a country router which then connects to the Gulf ISP Router. This topology allows ease of modifiability to the networks in the future.

A Cloud Router was connected to Qatar, Doha Router via redundant links. This cloud network had 5 application services implemented. The use of redundant links increases its availability as there is a lower chance of failure. These redundant links were made using Copper-Gigabit Ethernet due to the necessity of high speed between the cloud and the rest of the network. These services are accessible by all PCs at any time needed.

All connections between routers were carried out using Fibre-gigabit cables due to their long range compared to serial or copper connections. All connections within a LAN were made using Copper-Fast Ethernet cables. This choice was employed due to the devices within the LAN being closer in distance, hence negating the use of Fibre cables.

Every country has a single Dedicated DHCP server connected to a switch within that network. Kuwait and Bahrain's networks had the DHCP server set up in the router itself as per the project requirements. These DHCP servers assigned dynamic IP addresses in its own network and neighboring cities in Ajman, UAE and Damam, Saudia Arabia.

Cloud Network

This network had 5 Application Layer Services as follows:

1. DNS (Domain Name System):

- *Use:* DNS is crucial for translating human-readable domain names into IP addresses, facilitating seamless communication between devices on a network.

2. Web Server:

- *Use:* The Web Server service hosts websites. It is essential for simulating web-based applications and services within a network environment.

3. FTP (File Transfer Protocol):

- *Use:* FTP in Packet Tracer enables efficient and secure file transfer between devices on a network. This service is particularly valuable for sharing files, software updates, and configuration backups among network components.

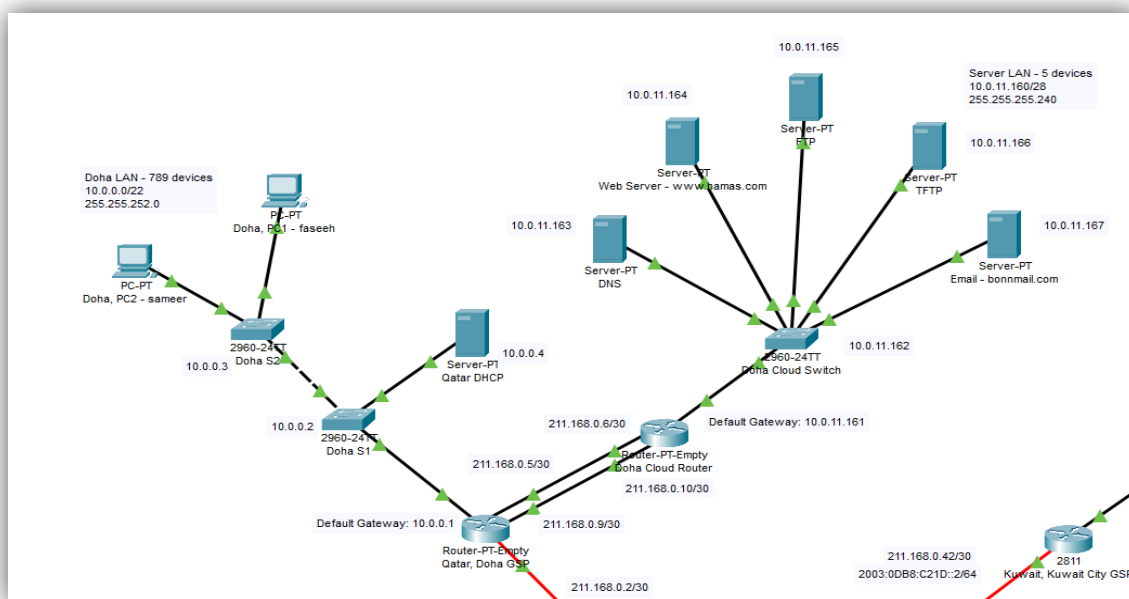
4. TFTP (Trivial File Transfer Protocol):

- *Use:* TFTP is a simplified version of FTP, commonly employed for lightweight file transfers. It is often utilized for network device configuration backups and updates due to its simplicity and efficiency.

5. Email:

- *Use:* The Email service manages electronic communication within the network. It facilitates the exchange of messages and files, allowing information sharing among devices in the network.

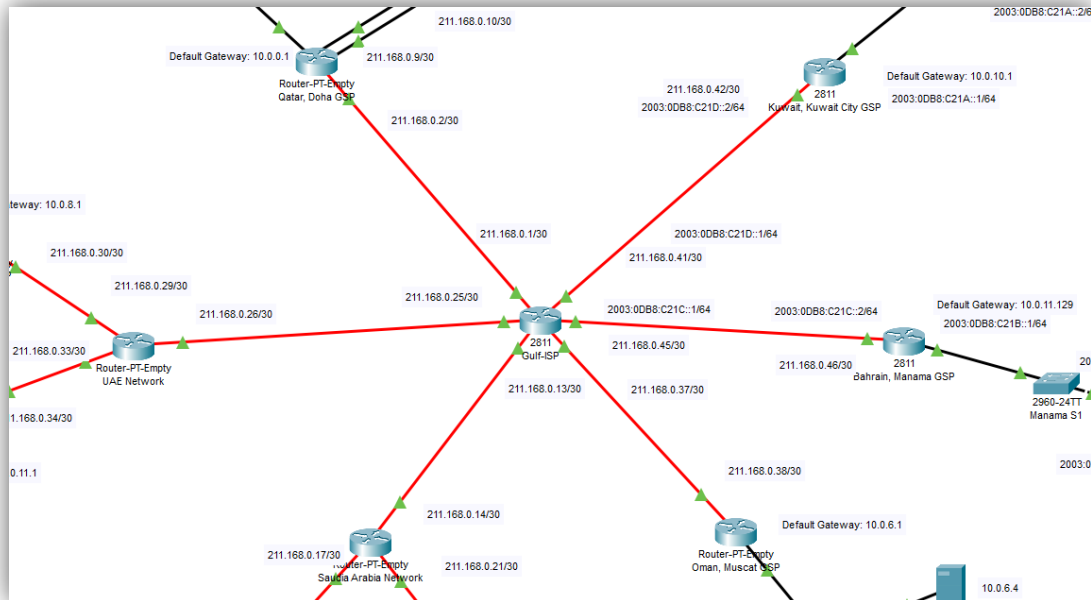
All application layer services are maintained on the cloud network. This network was directly connected to the Qatar GSP Building Router as per the instructions of the Project. They have redundant connections to ensure that backup is available in case one of the connections goes down.



Main Router Gulf ISP

We have a centralized connection of all GSP buildings through a core router, which is the Gulf-ISP, without direct links between buildings and the Qatar Headquarters.

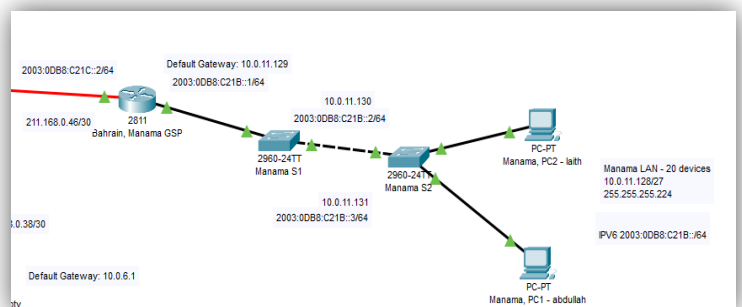
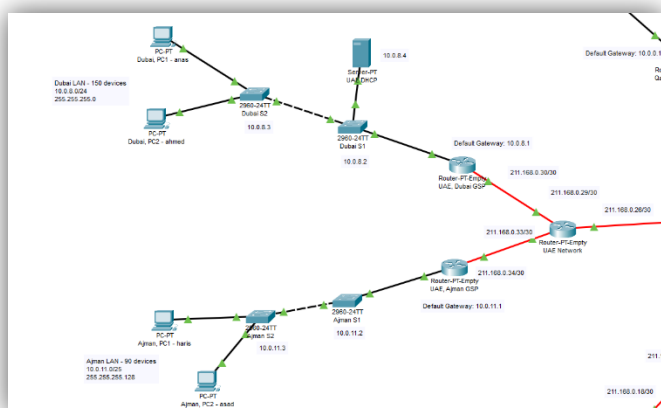
This setup promotes scalability, making it easier to expand the network or add new buildings without complex adjustments. Below is how we implemented the central router with all country routers connected to it.



DHCP Implementation

To implement DHCP services across the organization's various sites, we employed a dual-stack approach, utilizing both IPv4 and IPv6. In Kuwait and Bahrain, where both IP versions are utilized, the router functions as the DHCP server, efficiently assigning address for devices.

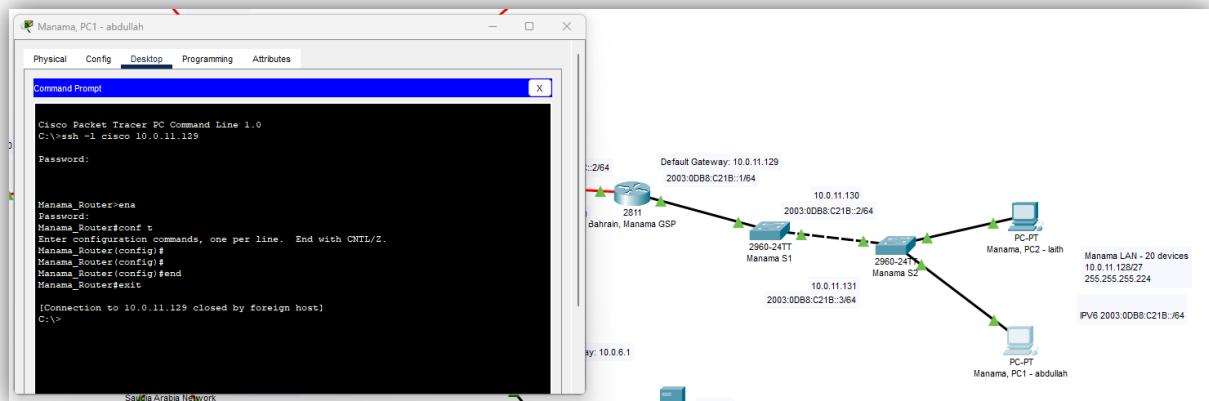
For other sites, dedicated DHCP servers are used, ensuring a centralized IP address allocation. Only one DHCP server was implemented per country, where countries with more than 1 city shared the same DHCP service via Relay Agent.



SSH Secure on Switches and Routers

To establish secure remote access across all switches and routers, SSH (Secure Shell) is implemented. SSH ensures a secure communication channel for remote management by encrypting the transmitted data. This setup enhances the overall security posture of the network infrastructure.

Each switch and router are configured to use SSH for remote access, providing a reliable and secure means for administrators to manage network devices remotely. By incorporating SSH into the configuration, sensitive information such as login credentials is encrypted, mitigating the risk of unauthorized access.



The above scenario shows connecting to Bahrain, Manama Router via SSH using the Manama, PC1 under the name Abdullah. SSH username and password is set to be **cisco** and using these credentials, we can alter the router information and make any necessary changes.

Static Routes

We configured static routes alongside dynamic routing protocols, our being RIP v2 and RIPng. Our protocol, RIP, has an administrative distance of 120. Hence, we provided an administrative distance of 125 to the static routes to make sure that RIP gets a higher priority every time.

In the event of dynamic routing failures or outages, these static routes act as a dependable backup, maintaining connectivity between locations and preventing potential network downtime.

