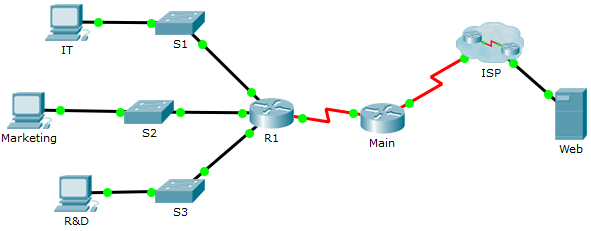
Packet Tracer – Troubleshooting Challenge

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IPv4 Address | Subnet Mask | Default Gateway |
| IPv6 Address/Prefix | IPv6 Link-local |
| R1 | G0/0 | 172.16.1.62 | 255.255.255.192 | N/A |
| 2001:DB8:CAFE::1/64 | FE80::1 | N/A |
| G0/1 | 172.16.1.126 | 255.255.255.192 | N/A |
| 2001:DB8:CAFE:1::1/64 | FE80::1 | N/A |
| G0/2 | 172.16.1.254 | 255.255.255.128 | N/A |
| 2001:DB8:CAFE:2::1/64 | FE80::1 | N/A |
| S0/0/1 | 10.0.0.2 | 255.255.255.252 | N/A |
| 2001:DB8:2::1/64 | FE80::1 | N/A |
| Main | S0/0/0 | 209.165.200.226 | 255.255.255.252 | N/A |
| 2001:DB8:1::1/64 | FE80::2 | N/A |
| S0/0/1 | 10.0.0.1 | 255.255.255.252 | N/A |
| 2001:DB8:2::2/64 | FE80::2 | N/A |
| S1 | VLAN 1 | 172.16.1.61 | 255.255.255.192 | 172.16.1.62 |
| S2 | VLAN 1 | 172.16.1.125 | 255.255.255.192 | 172.16.1.126 |
| S3 | VLAN 1 | 172.16.1.253 | 255.255.255.128 | 172.16.1.254 |
| IT | NIC | 172.16.1.1 | 255.255.255.192 | 172.16.1.62 |
| 2001:DB8:CAFE::2/64 | FE80::2 | FE80::1 |
| Marketing | NIC | 172.16.1.65 | 255.255.255.192 | 172.16.1.126 |
| 2001:DB8:CAFE:1::2/64 | FE80::2 | FE80::1 |
| R&D | NIC | 172.16.1.129 | 255.255.255.128 | 172.16.1.254 |
| 2001:DB8:CAFE:2::2/64 | FE80::2 | FE80::1 |
| Web | NIC | 64.100.0.3 | 255.255.255.248 | 64.100.0.1 |
| 2001:DB8:ACAD::3/64 | FE80::2 | FE80::1 |

1. Scenario / Background

After an update to the network, some devices were misconfigured. You have been tasked with correcting the configurations and verifying that all the PCs can access the websites, R1, switches, and other PC can access R1 using SSH.

Router R1 and all the switches have been preconfigured with the following:

* Enable password: **Ciscoenpa55**
* Console password: C**iscoconpa55**
* Admin username and password: **Admin1**/**Admin1pa55**

Required number of hosts per subnet:

* + IT: 50 hosts
  + Marketing: 50 hosts
  + R&D: 100 hosts

1. Requirements

* IT, Marketing, and R&D PCs can navigate to **www.cisco.pka** and **www.cisco6.pka**.
* IT, Marketing, and R&D PCs can SSH into R1 with the username **Admin1** and encrypted password **Admin1pa55**.
* All PCs should be able to ping R1, S1, S2, S3, and other PCs.