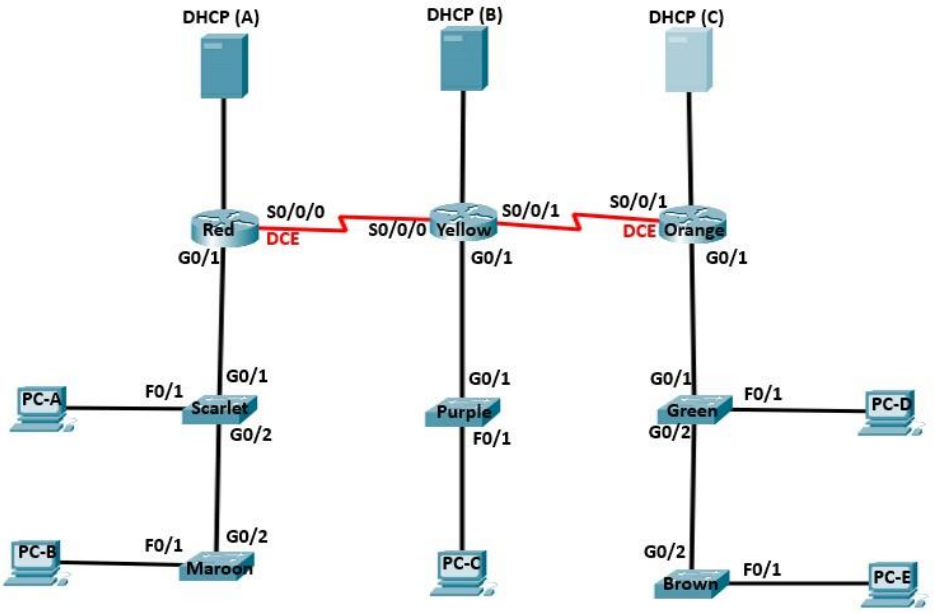
Cyber Briseno

Cisco Packet Tracer Project



Device	Interface	IP Address	Subnet Mask
RED	S0/0/0	30.30.30.1	255.255.255.252
	G0/0	192.168.1.1	255.255.255.0
	G0/1.10	99.99.10.1	255.255.255.0
	G0/1.20	99.99.20.1	255.255.255.0
	G0/1.99	99.99.99.1	255.255.255.0

Yellow	S0/0/0	30.30.30.2	255.255.255.252
	S0/0/1	30.30.30.5	255.255.255.252
	G0/0	192.168.2.1	255.255.255.0
	G0/1.30	99.99.30.1	255.255.255.0
	G0/1.99	99.99.100.1	255.255.255.0
	Lo1	15.15.15.15	255.255.255.255

Cyber Briseno
Cisco Packet Tracer Project

Orange	S0/0/1	30.30.30.6	255.255.255.252
	G0/0	192.168.3.1	255.255.255.0
	G0/1.40	99.99.40.1	255.255.255.0
	G0/1.50	99.99.50.1	255.255.255.0
	G0/1.99	99.99.101.1	255.255.255.0

Maroon	VLAN 10	99.99.10.10	255.255.255.0
	VLAN 20	99.99.20.10	255.255.255.0
	VLAN 99	99.99.99.10	255.255.255.0

Scarlet	VLAN 10	99.99.10.11	255.255.255.0
	VLAN 20	99.99.20.11	255.255.255.0
	VLAN 99	99.99.99.11	255.255.255.0

Purple	VLAN 30	99.99.30.10	255.255.255.0
	VLAN 99	99.99.100.10	255.255.255.0

Green	VLAN 40	99.99.40.10	255.255.255.0
	VLAN 50	99.99.50.10	255.255.255.0
	VLAN 99	99.99.101.10	255.255.255.0

Cyber Briseno

Cisco Packet Tracer Project

Brown	VLAN 40	99.99.40.11	255.255.255.0
	VLAN 50	99.99.50.11	255.255.255.0
	VLAN 99	99.99.101.11	255.255.255.0

DHCP Server (A)	NIC	192.168.1.100	255.255.255.0
DHCP Server (B)	NIC	192.168.2.100	255.255.255.0
DHCP Server (C)	NIC	192.168.3.100	255.255.255.0

Maroon	F0/1-11	VLAN 10	Emerald
	F0/12-24	VLAN 20	Silver
	N/A	VLAN 99	Management

Scarlet	F0/1-12	VLAN 20	Silver
	F0/13-24	VLAN 10	Emerald
	N/A	VLAN 99	Management

Purple	F0/1-24	VLAN 30	Fusion
	N/A	VLAN 99	Management

Green	F0/1-10	VLAN 40	Sunburst
	F0/11-24	VLAN 50	Blue
	N/A	VLAN 99	Management

Cyber Briseno
Cisco Packet Tracer Project

Brown	F0/1-10	VLAN 50	Blue
	F0/11-24	VLAN 40	Sunburst
	N/A	VLAN 99	Management

DHCP Server (A)

- Set the Static IP address, Subnet mask and Default Gateway
- Use the address table from above.
- Enable the DHCP Service
- Pool Name: Sunburst
- Set the default-gateway for the Sunburst network.
- Set the DNS server to 8.8.8.8
- Use the Sunburst network for your DHCP pool.
- Exclude the first 39 Usable IP addresses.
- Set the Subnet mask or Set the Maximum users to 110.

- Set the Static IP address, Subnet mask and Default Gateway
- Use the address table from above.
- Enable the DHCP Service
- Pool Name: Blue
- Set the default-gateway for the blue network.
- Set the DNS server to 8.8.8.8
- Use the Blue network for your DHCP pool.
- Exclude the first 39 Usable IP addresses.
- Set the Subnet mask or Set the Maximum users to 110.

DHCP Server (B)

- Set the Static IP address, Subnet mask and Default Gateway
- Use the address table from above.
- Enable the DHCP Service
- Pool Name: Emerald
- Set the default-gateway for the Emerald network.
- Set the DNS server to 8.8.8.8
- Use the Emerald network for your DHCP pool.
- Exclude the first 39 Usable IP addresses.

Cyber Briseno
Cisco Packet Tracer Project

- Set the Subnet mask or Set the Maximum users to 110.

- Set the Static IP address, Subnet mask and Default Gateway
- Use the address table from above.
- Enable the DHCP Service
- Pool Name: Silver
- Set the default-gateway for the silver network.
- Set the DNS server to 8.8.8.8
- Use the Silver network for your DHCP pool.
- Exclude the first 39 Usable IP addresses.
- Set the Subnet mask or Set the Maximum users to 110.

DHCP Server (C)

- Set the Static IP address, Subnet mask and Default Gateway
- Use the address table from above.
- Enable the DHCP Service
- Pool Name: Fusion
- Set the default-gateway for the Fusion network.
- Set the DNS server to 8.8.8.8
- Use the fusion network for your DHCP pool.
- Exclude the first 39 Usable IP addresses.
- Set the Subnet mask.
- Set the Maximum users to 110.

RED

- Assign the Hostname
- Disable DNS lookup.
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console.
- Encrypt all clear text passwords in current running configuration.
- Set a MOTD banner to “Configured by Briseno.”
- Configure SSH
  o Domain-Name: GitHub.com
  o Create a username of admin encrypted password of adminpass
  o Generate an RSA key with 1024 bits

Cyber Briseno
Cisco Packet Tracer Project

  - o Allow authentication with only the local database
  - o Enable only SSH access on VTY line
- Apply IP addresses according to the Addressing Table
- Disable CDP on S0/0/0
- Use a clock rate of 128000 on DCE interface.
- Configure Single-Area OSPFv2
  - o Process ID 100
  - o Area 0
  - o Router ID: 1.1.1.1
  - o Advertise all networks configured
  - o Apply passive interface on appropriate interfaces if applicable

Yellow

- Assign the hostname.
- Disable DNS lookup.
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console password.
- Encrypt all clear text passwords in current running configuration.
- Set a MOTD banner to “Configured by Briseno” o Configure SSH
- Domain-Name: GitHub.com
- Create a username of admin with an encrypted password of adminpass.
- Generate an RSA key with 1024 bits.
- Allow authentication with only the local database.
- Enable only SSH access on VTY line.
- Encrypt all plain text passwords.
- Apply IP addresses according to the Addressing Table
- Create loopback 1.
- Create a default route out of Lo1.
- Configure Single-Area OSPFv2
  - o Process ID 100
  - o Area 0
  - o Router ID: 2.2.2.2
  - o Advertise all networks configured
  - o Do not send OSPF updates out appropriate interfaces

Cyber Briseno
Cisco Packet Tracer Project

o Propagate the default route

- Configure NAT

o Configure a standard ACL numbered 20 to allow only the IP address within the 9.99.30.0/24 network.

o Configure NAT with a pool named AIT with the following range of public IP addresses:

o 200.56.53.200 to 200.56.53.250 with a subnet mask of 255.255.255.128

o Apply to the correct NAT interfaces.

Orange

- Assign the Hostname
- Disable DNS lookup.
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console password.
- Encrypt all clear text passwords in current running configuration.
- Set a MOTD banner to “Configured by Briseno.”
- Configure SSH
- Domain-Name: GitHub.com
- Create a username of admin with an encrypted password of adminpass.
- Generate an RSA key with 1024 bits.
- Allow authentication with only the local database.
- Enable only SSH access on VTY line.
- Apply IP addresses according to the Addressing Table
- Use a clock rate of 128000 on DCE interface.
- Configure Single-Area OSPFv2

  o Process ID 100

  o Area 0

  o Router ID: 3.3.3.3

  o Advertise all networks configured

  o Apply passive interface on appropriate interfaces if applicable

- Configure an Access Control List (ACL)

  o Create a standard ACL 65 to deny VLAN 50 from accessing VLAN 40

Cyber Briseno
Cisco Packet Tracer Project

o Permit all other traffic
o Apply to correct interface

Maroon

- Assign the Hostname
- Disable DNS lookup.
- Create a banner stating “Configured by Briseno.”
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console and vty password.
- Enable Telnet access only on VTY line.
- Encrypt all clear text passwords in current running configuration.
- Configure, name, and assign VLANs.
- Configure trunking.
- Set the default gateway with VLAN 99
- Configure Port Security
- Interface F0/1 only allow PC-B
- Configure Port Security on all other ports.
- DO NOT APPLY TO TRUNK INTERFACES
- Set maximum allowed MAC addresses to 3.
- Disable all unused interfaces.

Scarlet

- Assign the Hostname
- Disable DNS lookup.
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console and vty password.
- Enable Telnet access only on VTY line.
- Encrypt all clear text passwords in current running configuration.
- Set clock to current time.
- Create a banner stating “Configured by Briseno.”
- Configure, name, and assign VLANs.
- Configure trunking.
- Set the default gateway with VLAN 99
- Configure all ports assigned to VLANs as access ports.
- Configure Port Security o Interface F0/1 only allow PC-A

Cyber Briseno
Cisco Packet Tracer Project

- Configure Port Security on all other ports:
- DO NOT APPLY TO TRUNK INTERFACES
- o Set maximum allowed MAC addresses to three
- Disable all unused interfaces.

Purple

- Assign the Hostname
- Disable DNS lookup.
- Create a banner stating “Configured by Briseno.”
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console and vty password.
- Enable Telnet access only on VTY line.
- Encrypt all clear text passwords in current running configuration.
- Configure, name, and assign VLANs.
- Configure trunking.
- Set the default gateway with VLAN 99
- Configure Port Security
- Interface F0/1 only allow PC-C
- Configure Port Security on all other ports.
- DO NOT APPLY TO TRUNK INTERFACES
- Set maximum allowed MAC addresses to 3.
- Disable all unused interfaces.

Green

- Assign the Hostname
- Disable DNS lookup.
- Create a banner stating “Configured by Briseno.”
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console and vty password.
- Enable Telnet access only on VTY line.
- Encrypt all clear text passwords in current running configuration.
- Configure, name, and assign VLANs.
- Configure trunking.
- Set the default gateway with VLAN 99

Cyber Briseno
Cisco Packet Tracer Project

- Configure Port Security
- Interface F0/1 only allow PC-D
- Configure Port Security on all other ports.
- DO NOT APPLY TO TRUNK INTERFACES
- Set maximum allowed MAC addresses to 3.
- Disable all unused interfaces.

Brown

- Assign the Hostname
- Disable DNS lookup.
- Create a banner stating “Configured by Briseno.”
- Assign class as the Encrypted privileged EXEC mode password.
- Assign cisco as the console and vty password.
- Enable Telnet access only on VTY line.
- Encrypt all clear text passwords in current running configuration.
- Configure, name, and assign VLANs.
- Configure trunking.
- Set the default gateway with VLAN 99
- Configure Port Security
- Interface F0/1 only allow PC-E
- Configure Port Security on all other ports.
- DO NOT APPLY TO TRUNK INTERFACES
- Set maximum allowed MAC addresses to 3.
- Disable all unused interfaces.