SMALL SIZE COMPANY PROJECT

Daniel Garcia Gata

Contents

Introduction

Redundancy is essential for companies nowadays, a short moment of lost connection can be translated into a significant financial loss. This project focus on that exactly, finding the right topology to avoid this problem as much as possible without losing sight of the security aspect.

Scope of the project

This project has three main goals:

- Provide full redundancy with small possibility for the network to go offline at any moment.
- Provide secure access to Internet with routables IP addresses obtained dynamically and blocking communications between non allowed departments.
- SSH access for full monitoring and maintenance of the core network devices only by the maintenance department

Requirements

Functional requirements

- The three main departments of the company named Customer Service, Sales and Engineering, should have separate VLANs and they will be able to communicate between each other.
- The company must have a separate LAN for a Server Room and another one for the Maintenance department.

User requirements	Description
Location and number of workstations	• Sales department room has 10 workstations. • Customer service room has 8 workstations. • Engineering room has 5 workstations. • Maintenance room has 2 workstations. • Server room has one DHCP server plus another Backup DHCP server in the main area.
Availability	Full redundancy with small possibility of going offline.
Scalability	The network should be able to support any future expansions.
Security	Communications between LANs will be partially or totally limited for a certain services.

Network devices

Device	Quantity
Cisco 2911 Router	2
Cisco 2960-24TT Switch	6
DHCP Server	2
PC Workstation	25
Printer	3

IP address plan and VLANs

We were given the private IP address 192.168.1.0/24 for the main LAN (Sales, Customer service and Engineering departments) while the server room was given 10.1.1.0/28 and the Maintenance department obtained 10.1.2.0/28.

From the company requirements we need to divide the network 192.168.1.0/24 into 3 different subnets, the result will be this:

VLAN 10 – SALES (Availability for 30 hosts minimum)	
• Network address	• 192.168.1.64/26
• Subnet mask	• 255.255.255.192
• Broadcast address	• 192.168.1.127/26
• First usable address	• 192.168.1.65/26
• Last usable address	• 192.168.1.126/26
• Maximum number of hosts	• 62

VLAN 20 – CSERV (Availability for 35 hosts minimum)	
• Network address	• 192.168.1.0/26
• Subnet mask	• 255.255.255.192
• Broadcast address	• 192.168.1.63/26
• First usable address	• 192.168.1.1/26
• Last usable address	• 192.168.1.62/26
• Maximum number of hosts	• 62

VLAN 30 – ENGR (Availability for 15 hosts minimum)	
• Network address	• 192.168.1.128/27
• Subnet mask	• 255.255.255.224
• Broadcast address	• 192.168.1.159/27
• First usable address	• 192.168.1.129/27
• Last usable address	• 192.168.1.158/27
• Maximum number of hosts	• 30

Every end host of every subnet at the main LAN will obtain an IP address dynamically from the DHCP server located in the Server room while the Servers, Maintenance department hosts will have static IP addresses that are the following:

SERVER ROOM IP ADDRESSES	
DHCP-SRV1	10.1.1.1/28

MAINTENANCE DEPARTMENT IP ADDRESSES	
MAINTENANCE-PC1	10.1.2.1/28
MAINTENANCE-PC2	10.1.2.2/28

ROUTERS

Routing protocols

The routing protocol of choice for every LAN is OSPF as well as Floating static routes to ensure the connectivity in case OSPF fails. All VLANs will be aggregated using the supernet 192.168.1.0/24 in the same area (Area 0) with an administrative distance of 90 and auto-cost reference-bandwidth set to 10000. The floating static routes will be configured with an administrative distance of 120.

HSRP configuration

To ensure full redundancy, the network has two different routers but besides than that, HSRP has been enabled in both routers with a Virtual IP address that works as a Default Gateway for every host in every VLAN.

R1 – HSRP CONFIGURATION		
VLAN	Virtual IP	Priority
Standby 1 – VLAN 10	192.168.1.124/26	120
Standby 2 – VLAN 20	192.168.1.60/26	120
Standby 3 – VLAN 30	192.168.1.156/27	120

R2 – HSRP CONFIGURATION		
VLAN	Virtual IP	Priority
Standby 1 – VLAN 10	192.168.1.124/26	90
Standby 2 – VLAN 20	192.168.1.60/26	90
Standby 3 – VLAN 30	192.168.1.156/27	90

Router Interface information

R1			
Interface	IP address	Status	Connected to
G0/0	-	Up/Up	SW2's G0/1
G0/0.10 (VLAN10)	192.168.1.126/26	Up/Up	
G0/0.20 (VLAN20)	192.168.1.62/26	Up/Up	
G0/0.30 (VLAN30)	192.168.1.158/27	Up/Up	
G0/1	203.0.112.1/30	Up/Up	INTERNET
G0/2	10.1.1.14/28	Up/Up	SW5's G0/1

R2			
Interface	IP address	Status	Connected to
G0/0	-	Up/Up	SW4's G0/1
G0/0.10 (VLAN10)	192.168.1.125/26	Up/Up	
G0/0.20 (VLAN20)	192.168.1.61/26	Up/Up	
G0/0.30 (VLAN30)	192.168.1.157/27	Up/Up	
G0/1	203.0.113.1	Up/Up	INTERNET
G0/2	10.1.2.14/28	Up/Up	SW6's G0/1

Switches

SW1			
Interface	Status	Connected to	STP Role
F0/1	Up/Up	CSERV-PC1	Designated (Portfast enabled)
F0/2	Up/Up	CSERV-PC2	Designated (Portfast enabled)
F0/3	Up/Up	CSERV-PC3	Designated (Portfast enabled)
F0/4	Up/Up	CSERV-PC4	Designated (Portfast enabled)
F0/5	Up/Up	CSERV-PC5	Designated (Portfast enabled)
F0/6	Up/Up	CSERV-PC6	Designated (Portfast enabled)
F0/7	Up/Up	CSERV-PC7	Designated (Portfast enabled)
F0/8	Up/Up	CSERV-PC8	Designated (Portfast enabled)
F0/9	Up/Up	CSERV-PRINTER	Designated (Portfast enabled)
F0/10	Up/Up	SW2's F0/7	Root
F0/11	Up/Up	SW4's F0/2	Designated
F0/12	Up/Up	SW3's F0/14	Designated
F0/13 to F0/24	Administratively down/Down	-	-
G0/1 // G0/2	Administratively down/Down	-	-

SW2			
Interface	Status	Connected to	STP Role
F0/1	Up/Up	ENGR-PC1	Designated (Portfast enabled)
F0/2	Up/Up	ENGR-PC2	Designated (Portfast enabled)
F0/3	Up/Up	ENGR-PC3	Designated (Portfast enabled)
F0/4	Up/Up	ENGR-PC4	Designated (Portfast enabled)
F0/5	Up/Up	ENGR-PC5	Designated (Portfast enabled)
F0/6	Up/Up	ENGR-PRINTER	Designated (Portfast enabled)
F0/7	Up/Up	SW1's F0/10	Designated
F0/8	Up/Up	SW3's F0/13	Designated
F0/9	Up/Up	SW4's F0/3	Designated
F0/10 to F0/24	Administratively down/Down	-	-
G0/1	Up/Up	R1's G0/0	-
G0/2	Administratively down/Down	-	-

SW3			
Interface	Status	Connected to	STP Role
F0/1	Up/Up	SALES-PC1	Designated (Portfast enabled)
F0/2	Up/Up	SALES-PC2	Designated (Portfast enabled)
F0/3	Up/Up	SALES-PC3	Designated (Portfast enabled)
F0/4	Up/Up	SALES-PC4	Designated (Portfast enabled)
F0/5	Up/Up	SALES-PC5	Designated (Portfast enabled)
F0/6	Up/Up	SALES-PC6	Designated (Portfast enabled)
F0/7	Up/Up	SALES-PC7	Designated (Portfast enabled)
F0/8	Up/Up	SALES-PC8	Designated (Portfast enabled)
F0/9	Up/Up	SALES-PC9	Designated (Portfast enabled)
F0/10	Up/Up	SALES-PC10	Designated (Portfast enabled)
F0/11	Up/Up	SALES-PRINTER	Designated (Portfast enabled)
F0/12	Up/Up	SW4's F0/1	Designated
F0/13	Up/Up	SW2's F0/8	Root
F0/14	Up/Up	SW1's F0/12	Alternate
F0/15 to F0/24	Administratively down/Down	-	-
G0/1 // G0/2	Administratively down/Down	-	-

SW4			
Interface	Status	Connected to	STP Role
F0/1	Up/Up	SW3's F0/12	Alternate
F0/2	Up/Up	SW1's F0/11	Alternate
F0/3	Up/Up	SW2's F0/9	Root
F0/4 to F0/24	Administratively down/Down	-	-
G0/1	Up/Up	R1's G0/1	-
G0/2	Up/Up	DHCP-BACKUP	-

SW5		
Interface	Status	Connected to
F0/1	Administratively down/Down	-
F0/2 to F0/24	Administratively down/Down	-
G0/1	Up/Up	R1's G0/2
G0/2	Up/Up	DHCP-SRV1

SW6		
Interface	Status	Connected to
F0/1	Up/Up	MAINTENANCE-PC1
F0/2	Up/Up	MAINTENANCE-PC2
F0/3 to F0/24	Administratively down/Down	-
G0/1	Up/Up	R2's G0/2
G0/2	Administratively down/Down	-

DHCP Configuration

Every end host will be able to obtain an IP address dynamically from the main DHCP server located at 10.1.1.0/28 network. There is also a back up DHCP server in case R1 shuts down or the main DHCP Server fails. Every VLAN has a IP address pool as it shows below:

VLAN	IP Address Range	Excluded IP addresses	Maximum number of users
VLAN 10 - SALES	192.168.1.65-192.168.1.95	192.168.1.106-192.168.1.126	30
VLAN 20 - CSERV	192.168.1.1-192.168.1.36	192.168.1.42-192.168.1.62	35
VLAN 30 - ENGR	192.168.1.129-192.168.1.144	192.168.1.145-192.168.1.158	15

NAT Configuration

Every VLAN has 2 different NAT pools assigned, one for every router, the routable IP address are as follows:

Router	VLAN	Pool name	IP address range	Netmask
R1	10	POOL_SALES	50.0.0.0 – 50.0.0.30	255.255.255.192
R2	10	POOL_SALES2	40.0.0.0 – 40.0.0.30	255.255.255.192
R1	20	POOL_CSERV	100.0.0.0 – 100.0.0.35	255.255.255.192
R2	20	POOL_CSERV2	90.0.0.0 – 90.0.0.35	255.255.255.192
R1	30	POOL_ENGR	25.0.0.0 – 25.0.0.20	255.255.255.224
R2	30	POOL_ENGR2	15.0.0.0 – 15.0.0.20	255.255.255.224

ACLs (Standard and Extended)

R1 configured ACLs

- Interface G0/0.10
  - Permit OSPF protocol to any
  - Deny access to network 192.168.1.128 from network 192.168.1.64 (with subnet mask /26)
  - Permit access to host 10.1.1.1 from network 192.168.1.64 (with subnet mask /26)
  - Permit access to network 203.0.112.0 from network 192.168.1.64 (with subnet mask /26)
  - Permit UDP access from port 1985 (HSRP) to any
  - Permit any access

- Interface G0/0.20
  - Permit OSPF protocol to any
  - Deny access to network 192.168.1.128 from network 192.168.1.0 (with subnet mask /26)
  - Permit access to host 10.1.1.1 from network 192.168.1.0 (with subnet mask /26)
  - Permit access to network 203.0.112.0 from network 192.168.1.0 (with subnet mask /26)
  - Permit UDP access from port 1985 (HSRP) to any
  - Permit any access

- Interface G0/0.30
  - Permit OSPF protocol to any
  - Permit access to host 10.1.1.1 from network 192.168.1.128 (with subnet mask /27)
  - Permit access to network 203.0.112.0 from network 192.168.1.128 (with subnet mask /27)
  - Permit UDP access from port 1985 (HSRP) to any
  - Permit any access

- Interface G0/2
  - Permit OSPF protocol to any
  - Permit access to network 192.168.1.0 (with subnet mask /24) from host 10.1.1.1
  - Permit access to host 10.1.2.1 from host 10.1.1.1
  - Permit access to host 10.1.2.2 from host 10.1.1.1
  - Permit access to network 203.0.112.0 from network 10.1.1.0 (with subnet mask /28)
  - Permit any access

R2 configured ACLs

- Interface G0/0.10
  - Permit OSPF protocol to any
  - Denied access to network 192.168.1.128 from network 192.168.1.64 (with subnet mask /26)
  - Permit UDP access from port 1985 (HSRP) to any
  - Permit access to network 203.0.113.0 from network 192.168.1.64 (with subnet mask /26)
  - Permit any access

- Interface G0/0.20
  - Permit OSPF protocol to any
  - Permit UDP access from port 1985 (HSRP) to any
  - Denied access to network 192.168.1.128 from network 192.168.1.0 (with subnet mask /26)
  - Allow access to host 10.1.1.1 from network 192.168.1.0 (with subnet mask /26)
  - Permit access to network 203.0.113.0 from network 192.168.1.0 (with subnet mask /26)
  - Permit any access

- Interface G0/0.30
  - Permit OSPF protocol to any
  - Permit UDP access from port 1985 (HSRP) to any
  - Allow access to host 10.1.1.1 from network 192.168.1.128 (with subnet mask /27)
  - Permit access to network 203.0.113.0 from network 192.168.1.128 (with subnet mask /27)
  - Permit any access

- Interface G0/2
  - Permit OSPF protocol to any
  - Allow access to network 192.168.1.0 (with subnet mask /24) from host 10.1.2.1
  - Allow access to network 192.168.1.0 (with subnet mask /24) from host 10.1.2.2
  - Allow access to host 10.1.1.1 from host 10.1.2.1
  - Allow access to host 10.1.1.1 from host 10.1.2.2
  - Permit access to network 203.0.112.0 from network 10.1.2.0 (with subnet mask /28)
  - Permit SSH access for host 10.1.2.1
  - Permit SSH access for host 10.1.2.2
  - Deny SSH access for any
  - Permit any access

SSH Configuration

Every network device will be controlled via SSH by the end hosts of the network 10.1.2.0/28, exclusively by hosts 10.1.2.1 and 10.1.2.2 (MAINTENANCE-PC1 and MAINTENANCE-PC2). The password and username is:

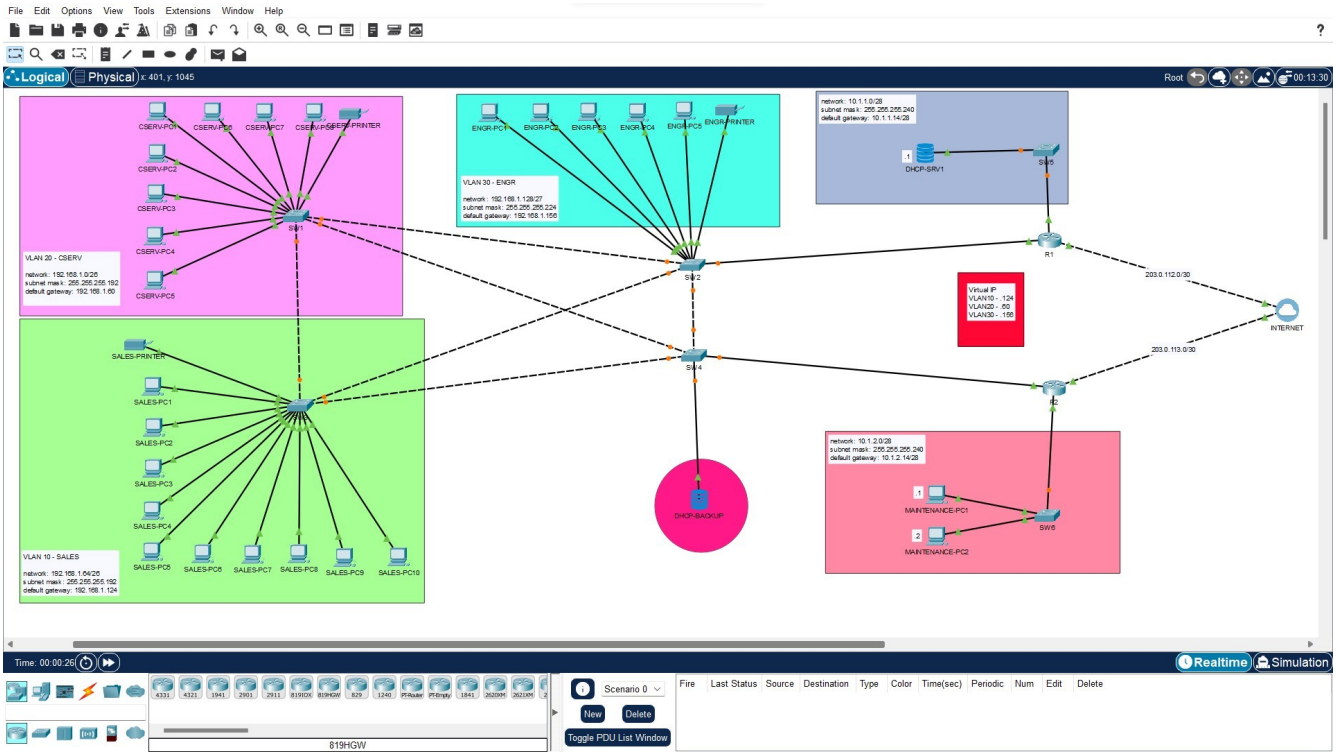
- Username: admin
- Password: cisco

The list of network devices that have SSH access enabled are:

- DHCP-SRV1
- DHCP-BACKUP
- R1
- R2
- SW6
- SW5

Logic Interfaces and IP addresses for SSH			
Device	Interface	IP address	Subnet mask
SW5	VLAN1	10.1.1.2	255.255.255.240
SW6	VLAN1	10.1.2.3	255.255.255.240

Network Topology Diagram



Summary

In this project, I wanted to try different subjects like providing full redundancy using a Virtual IP as a default gateway using HSRP, DHCP and Dynamic NAT as well as SSH configuration or Extended and Standard ACL's. This way I could design a topology that has a reliable connectivity and it has dynamic services providing IP addresses and routable IP addresses to be able to connect to internet.