**Sunrise Network Project**

The goal of this project was to create a functioning, simulated campus network environment in Packet Tracer while implementing many of the concepts, technologies and protocols learned from studying for the CCNA (Cisco Certified Network Associate) course and exam. The company, Sunrise Inc., is fictional and the campus is based on a call-center structure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Department | Hostname | VLAN | Address | Subnet |
| **Customer Service** | PC1 | 10 | 192.168.1.1 | 192.168.1.0 /24 |
| PC2 | 192.168.1.2 |
| **Collections** | PC3 | 20 | 192.168.2.1 | 192.168.2.0 /24 |
| PC4 | 192.168.2.2 |
| **Global Support** | PC5 | 30 | 192.168.3.1 | 192.168.3.0 /24 |
| PC6 | 192.168.3.2 |
| **HR** | PC7 | 40 | 192.168.4.1 | 192.168.4.0 /24 |
| PC8 | 192.168.4.2 |
| **Management** | PC9 | 50 | 172.16.5.1 | 172.16.5.0 /24 |
| PC10 | 172.16.5.2 |
| **Security** | PC11 | 60 | 172.16.6.1 | 172.16.6.0 /24 |
| PC12 | 172.16.6.2 |
| **Services** | DHCPSRV |  | 10.0.0.1 | 10.0.0.0 /29 |
| DNSSRV | 10.0.0.2 |
| NTPSRV | 10.0.0.3 |
| SYSLOGSRV | 10.0.0.4 |
| Admin | 10.0.0.5 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Management** | WLC | 70 | 10.7.0.1 | 10.7.0.0/24 |
| **Internal** | WLC | 80 | 172.16.8.1 | 172.16.8.0/24 |
| **Guest** | WLC | 90 | 192.168.9.1 | 192.168.9.0/24 |

* VLANs
* STP Bridge Load-Balancing
* Etherchannel
* Floating Static Routes
* OSPF
* IPV6
* Access-lists
* HSRP
* CDP
* DNS
* NTP
* DHCP
* SNMP
* SSH
* NAT
* Port Security
* DHCP Snooping
* DAI
* **Initial Layout**
* Call-center campus
* 3-tier infrastructure (Access, Distribution, Core)
* Designated Services VLAN/Subnet
* Edge router connected to ISP
* **IPv4/IPv6 addressing, LANS, Etherchannel, trunks/ROAS**

6 departments; ***Customer Service, Collections, Global Support, HR, Management, Security*** + 1 ***Services*** segment with assigned VLANs (10 – 60) and subnets based on common, private IP address formats. IPv6 addressing to reflect IPv4 subnet schemes; utilized EUI-64 to create unique IPv6 addresses. Static Etherchannel configured between CSW1 & CSW2. Trunk/ROAS configured between access switches and distribution layer switches/routers. Created loopback interfaces on network devices for redundancy.

* **Access-Layer Security**
* Enabled console/enable password on all network devices
* Enabled **Portfast** + **BPDU Guard** on all edge/client switchports
* Disabled **DTP**/manually configure access ports
* Moved unused access ports to unused VLAN (150)
* Changed default native VLAN on trunk ports to unused VLAN (100)
* Manually disabled unused ports
* Enabled **Port-Security** on active access ports (***Violation Mode****: Shutdown,* ***1 Maximum address***)
* **DHCP snooping** – Enabled globally + active VLANs. Configured uplink ports as trusted. Disabled DHCP Information Option 82.
* **Dynamic Arp Inspection** – Enabled on active VLANS. Configured uplink ports as trusted.
* **OSPF/OSPFv3**

Enabled OSPFv2 for all IPv4 subnets + loopback interfaces. Utilized *network/wildcard* commands and/or enabled directly on interfaces. Enabled OSPFv3 for all IPv6 subnets. Configured passive-interfaces.

* **HSRP**

**HSRP** (Hot Standby Router Protocol) version 2 configured on each distribution-layer router subinterface; providing gateway redundancy for each VLAN/subnet. Manually adjusted priority and enabled preemption.

* **DHCP | Configure/Perform**

**DHCP** server *(DHCPSRV)* added to ***Services*** segment. Configured address pool for each department. Performed **DHCP** IP requests from each PC to have IPv4 address automatically assigned.

* **DNS Server**

Added **DNS** server *(DNSSRV)* to ***Services*** segment and configured A Records for each network device.

*\*PC A records added after performing initial DHCP IP assignment and may not correspond to current DHCP IP assignments. No IP reservation feature available. Can be mitigated by utilizing static IP addressing.*

* **NTP**

Added dedicated **NTP** (Network Time Protocol) server *(NTPSRV)* to ***Services*** segment; set as NTP Master/Stratum 1. Enabled authentication and created authentication-key (1): ***sunrise.*** Updated hardware calendar. Configured **NTP** on all routers and set *NTPSRV* as primary server using authentication-key.

* **Syslog**

Added **Syslog** server *(SYSLOGSV)* to ***Services*** segment. Configured routers to send log messages externally to *SYSLOGSRV* with severity level set to 7 (debugging)

* **ACLs (Access-Control Lists)**

Created standard-numbered ACL **1** to limit ***Services*** segment access to local network subnets and devices using wildcard masks and device loopback interface host addresses. Applied to DR5/DR6 in outgoing direction on interfaces that connect to ***Services*** VLAN/Subnet. Created standard-numbered ACL **99** on all routers to restrict VTY line access to ***Admin*** PC located in the ***Services*** segment.

* **NAT**

Configured PAT/NAT Overload on ***Edge*** router. Defined inside/outside interfaces. Created standard ACL ***TRANSLATE*** to define subnets containing end devices by utilizing wildcard masks. Configured router to translate addresses specified by ACL to IP address of outside interface.

* **Default Route | Configure + Advertise**

Configured default route to ISP on ***Edge*** router. Advertised default route to all other network routers via OSPF using the ***default information originate*** command.

* **SSH**

Configured SSH Version 2 on all network routers. Defined domain-name and generated RSA keys. Enabled *privileged exec* mode password. Created username/password for admin and enabled local login for console line and VTY lines. Created/applied ACL **99** to limit SSH access to admin PC. Limited VTY line access to SSH only.

* + Enable secret: sunrise
  + **Username**: admin **Password**: sunrise
  + Domain Name: sunrise.com
  + Enabled Version 2
  + Created/Applied ACL 99 to VTY lines
  + Restricted VTY to SSH only
* **WLC/WLANs/APs**

Added WLC, APs and multi-layer switch dedicated for wireless purposes. Created VLANs 70, 80 and 90 for use with Management, Internal and Guest WLANs. Created dedicated SVIs for each VLAN to act as default gateways and perform inter-VLAN routing. Enabled/defined individual DHCP pools for use with Internal & Guest clients.

**Challenges**

* **Services IPV6 subnet not appearing in OSPF**

\*Fixed by disabling/reenabling OSPFv3.

* **Enabling ROAS on multi-layer switch (NTP, SSH)**

\*Received error message when attempting to create subinterfaces on multi-layer switches. Swapped multi-layer switches DR1, DR2, DR3, DR4 for standard routers.

* **Default gateway via ROAS for access switches.**

\*Attempted to configure SVI for standard access switches for use with SSH, NTP etc. Unsure of necessary default-gateway/ROAS configuration.

* **Access-list issues with ISP router, loopback interfaces.**

\*Failed pings from ***Services***subnet to ***ISP*** router + loopback interfaces. Returned pings being blocked by access-list. Created additional entries to enable communication.

* **Services subnet unable to ping DR6 loopback (6.6.6.6)**

\*Services subnet (10.0.0.0/8) being blocked by outgoing ACL after first traveling to active default gateway (DR5). Created additional ACL entry for subnet.

* **DNS may not work for PCs due to DHCP configuration.**

\*PC A records added after performing initial DHCP IP assignment and may not correspond to current DHCP IP assignments. No IP reservation feature available. Can be mitigated by utilizing static IP addressing.

* **Receiving** *Server Reset Connection***error when attempting to access/configure WLC GUI.**

\*Ensured using HTTPS and verified configurations. Unsure if issue related to Packet Tracer. Swapped WLC with WLC-PT to allow direct device configuration.