ENCOR - University lab

This is a lab that builds a network in different phases. As an example we are using a imaginary university network. Some of the skills needed are (but not excluded to):

- spanning tree + security
- etherchannel
- vlans
- fhrp protocols
- static routing
- ospf
- bgp
- ipv6
- ntp
- syslog
- ipsec
- vrf
- nat
- ...

> **BEWARE:** This design does not follow best practices. Shortcuts were taken (and other crappy solutions) in order to stay under the 20 node limit in cml.

The lab follows an organic approach where you are tasked bit by bit to expand the existing network.

How to use this repo

The cml lab can be found in the `cml` directory. The lab is fully built and includes (basic) default configurations for all devices. There is also a fully built and configured lab provided.

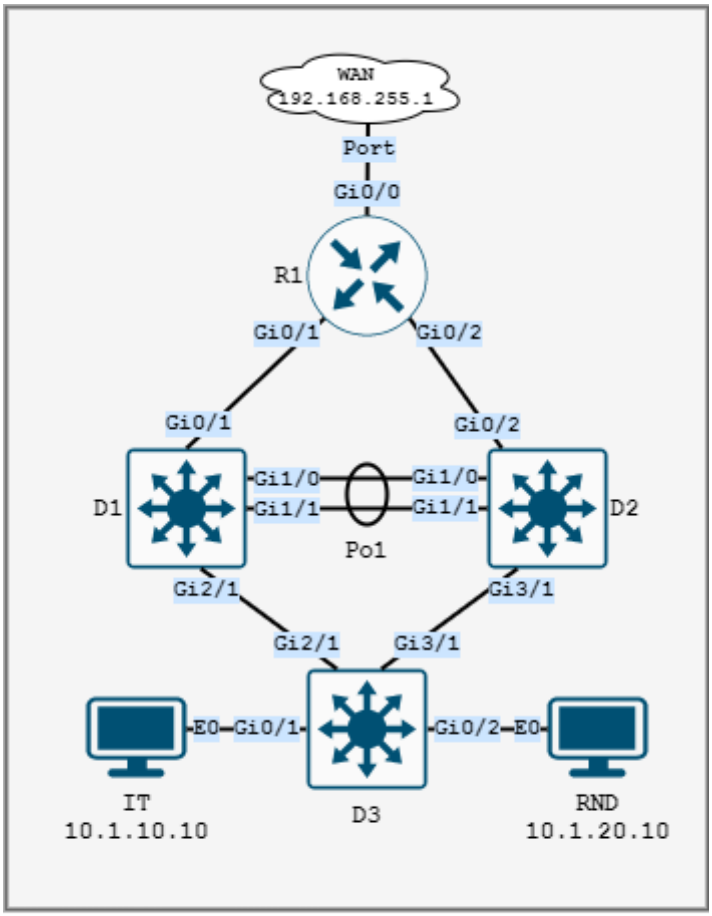
All drawings and other assets can be found in the `assets` directory.

Network design overview

The network uses the following supernet and considerations:

- For IPv4 `10.0.0.0/8` is used as the supernet as `10.building.vlan.ip`
- For IPv6 `2001:db8::/64` is used as the supernet as `2001:db8:building:vlan::ip`
- The network has been assigned `AS65200`
- Gateways are always the first usable ip in each range
- Vlan `30` is used for switch management
- Subnet `40` is used on each site for router management

Phase 1



Building 1
10.1.0.0/16
2001:db8:1::/64

The university has tasked you to deploy the network for building `1`. You will need to provide the following vlans:

```
IT vlan 10 - 10.1.10.0/24
RND vlan 20 - 10.1.20.0/24
MGMT vlan 30 - 10.1.30.0/24
NATIVE vlan 999
```

Switches D1 and D2 are connected via etherchannel using the `LACP` protocol.

Build all trunks between the switches. Disable `DTP` and use `dot1q` encapsulation. Do not use a dynamic trunking protocol and force the ports into `trunk` mode. Allow only the necessary vlans.

Use `rapid-pvst` as the spanning-tree protocol. Make sure to take the following requests in account:

- D1 is the root bridge for all client vlans (10,20) and D2 is the secondary root bridge
- Use root guard on all necessary ports on D1 and D2
- Use portfast for all edge ports and enable bpduguard on D3

Provide management access to all switches in the mgmt vlan (30). Use the following ip addresses:

```
D1 - 10.1.30.21
D2 - 10.1.30.22
D3 - 10.1.30.23
```

Allow management via ssh version 2:

- use the domain name `uni.local`
- username `uni` password `admin`
- `2048 bit` keys.
- Use Use an acl to only allow the IT vlan to access the switches via ssh. Name the acl `MGMT_IT`.

Provide a redundant gateway for the IT and RND vlan on D1 and D2. Use `HSRP` version 2 with the following parameters:

- hello and hold timer of 1 and 3 seconds
- authentication plaintext string `fail0ver`
- the hsrp group number equals the vlan id
- D1 has the `10.1.x.251` ip and D2 has the `10.1.x.252` ip for each vlan
- The gateway is `10.1.x.1`
- Enable preemption with a delay of `30` seconds
- D1 has a priority of `150` and D2 has a priority of `130`

Setup management for R1. Use interface `Lo40` with ip address `10.1.40.10`.

Setup routed ports between R1 and D1/D2. Use the following ip addresses:

```
D1 - G0/1 - 10.1.11.2/30
D2 - G0/2 - 10.1.11.6/30
R1 - G0/1 - 10.1.11.1/30
R1 - G0/2 - 10.1.11.5/30
```

Setup a fully specified, default static route for D1 and D2 pointing to R1.

On R1 setup fully specified default static routes to D1 and D2 for the `10.1.0.0/8` network. Give the route to D1 a metric of `1` and the route to D2 a metric of `2`.

Connect R1 to the WAN. Use `192.168.255.2/24` as the ip address on interface `G0/0`. Setup a fully specified default static route pointing to the WAN with a metric of 150.

Let R1 use `9.9.9.9` and `8.8.8.8` as domain servers.

Setup ntp on R1 and sync to `pool.ntp.org`. Setup R1 as a ntp master for the network with a stratum value of `4`.

Setup ntp on D1, D2 and D3 to use `10.1.40.10` as their ntp server.

Setup PAT for the `10.1.0.0/16` network. Don't allow RND access to the internet. Name the acl `PAT_10_1_0_0`.

Track the line protocol for interface `g0/1` on D1. If the protocol goes down decrement the hsrp priority with `40`. Use tracking group `5`.

Phase 2

IPv6 rollout for internal networks. vlan interfaces use ipv6 for client networks. setup hsrp for client networks for ipv6

add static ipv6 routes on D1, D2 and R1

Phase 3

another building is built with subnet `10.2.0.0`. Ospf routing and summarization. The building contains 2 lab environments with overlapping subnets. provide a vrf for each lab environment and provide PAT for each lab network

Phase 4

2 bgp routers on the network edge. use route maps to prefer one inbound path via as_path prepending and make sure that our network does not become a transit network

Phase 5

A remote office was added. Use one router with a loopback and ipsec. aaa rolout for the network

Startup configurations

Endpoints

IT

```
# this is a shell script which will be sourced at boot
hostname IT
ip link set dev eth0 up
ip address add 10.1.10.10/24 dev eth0
ip route add default via 10.1.10.1
ip -6 address add 2001:db8:1:10::10/64 dev eth0
echo 'nameserver 9.9.9.9' > /etc/resolv.conf
# configurable user account
USERNAME=cisco
PASSWORD=cisco
```

RND

```
# this is a shell script which will be sourced at boot
hostname RND
ip address add 10.1.20.10/24 dev eth0
ip link set dev eth0 up
ip route add default via 10.1.20.1
ip -6 address add 2001:db8:1:20::10/64 dev eth0
echo 'nameserver 9.9.9.9' > /etc/resolv.conf
# configurable user account
USERNAME=cisco
PASSWORD=cisco
```

Routers

R1

```
hostname R1
no logging console

line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 logging synchronous
 login
line vty 5 15
 exec-timeout 0 0
 logging synchronous
 login
end
```

Switches

D1

```
hostname D1
no logging console

line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 logging synchronous
```

```
 login
line vty 5 15
 exec-timeout 0 0
 logging synchronous
 login
end
```

D2

```
hostname D2
no logging console

line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 logging synchronous
 login
line vty 5 15
 exec-timeout 0 0
 logging synchronous
 login
end
```

D3

```
hostname D3
no logging console

line con 0
 exec-timeout 0 0
 logging synchronous
```

```
line vty 0 4
 exec-timeout 0 0
 logging synchronous
 login
line vty 5 15
 exec-timeout 0 0
 logging synchronous
 login
end
```