Scalable Network Design for Schools

Recommended Network Design Practices

Ronald Matovu
rmatovu@renu.ac.ug

Recommended Network Design Practices

14th May 2023

Enabling Research & Education Collaboration

Outline

- Design practices
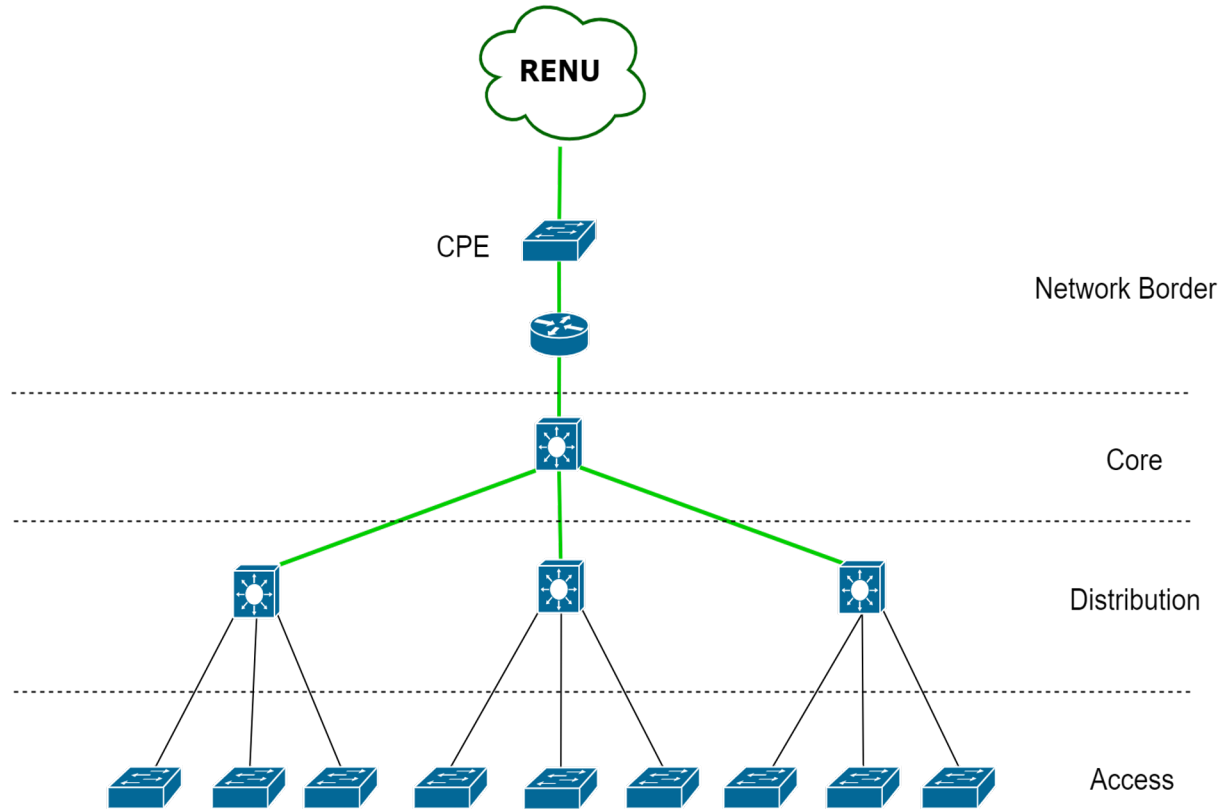
- Summary

- Scenario

Hierarchical network design model

Using a hierarchical network design model that consists of three layers: core, distribution and access with separation of functions.
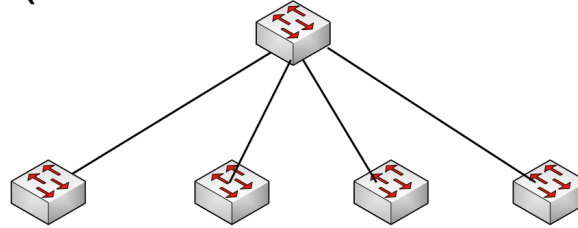
This model provides;

- Modularity
- Resilience
- Flexibility
- Scalability

RENU

CPE

Network Border

Core

Distribution

Access

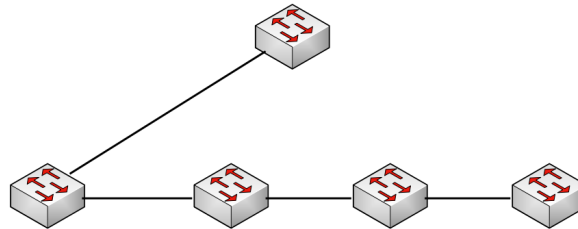Enabling Research & Education Collaboration

Minimize Number of Network Devices in the Path

- Build hub and spoke (sometimes called star) networks

- Not daisy chained (sometimes called cascaded) networks

Hub and Spoke Design

- We will use this design pattern in two places in our network

  1. Between Buildings. We will run fiber optic cabling from a central location in a hub-and-spoke fashion to each remote building

  2. Inside of each building. We will run unshielded twisted pair (and possibly fiber) from the main rack in each building to all other racks.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Hub and Spoke at Campus Level

- At the campus level, best practices are to build hub and spoke networks

- The hub at the campus level is often called the core

- Best practices are to route at the core
  - This segments the network into independent subnets
  - Limits broadcasts

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Hub and Spoke Networks Inside of Buildings

- Inside of each building, we will also build a hub and spoke network.
- This hub and spoke network is what provides Service to end users
- Each of these networks will be an IP subnet
- Plan for no more than 250 Computers at maximum
- Should be one of these for every reasonable sized building
- This network should only be switched
- Often, the in-building portion is called the Edge of your network
- Always buy switches that are managed
  – no unmanaged switches!

Putting it all Together
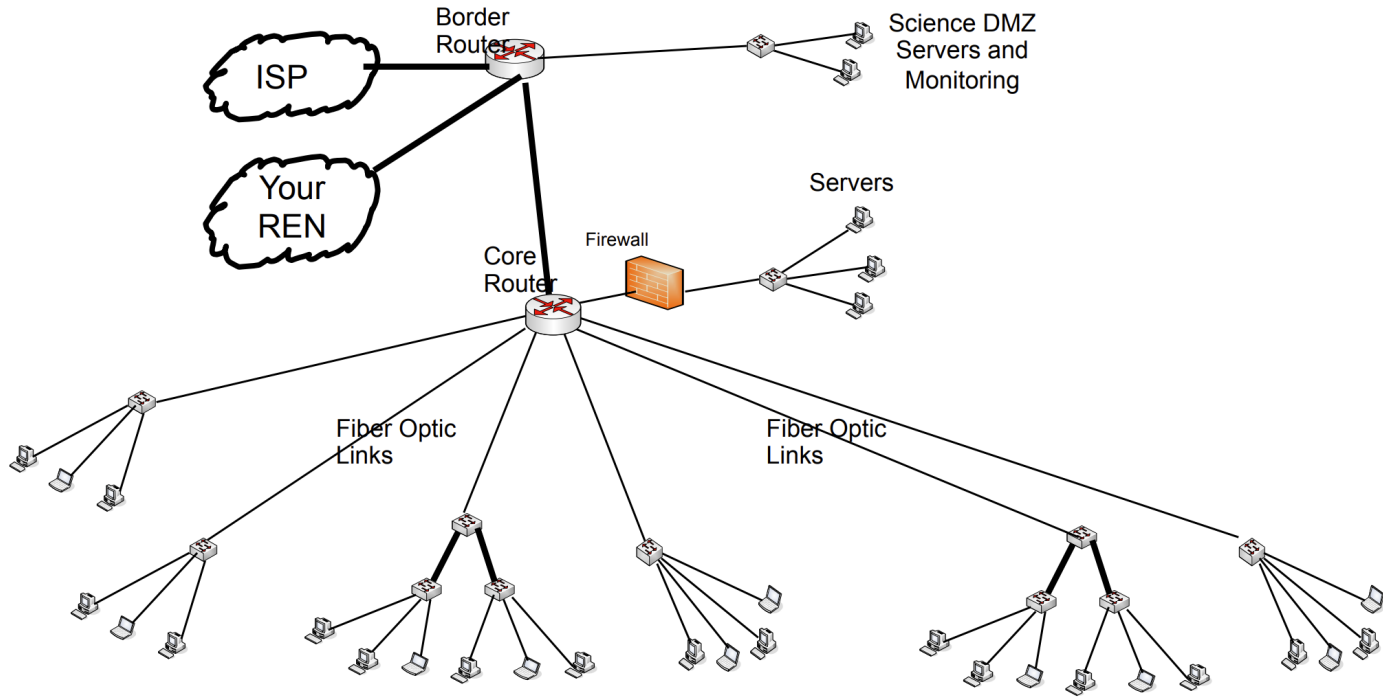
Choose appropriate devices

- Routers

- Layer 2 or layer 3 switches

- Firewalls

- Buy devices that support SNMP

Use Redundant Links

Using redundant links and devices at each layer to provide high availability and fast convergence in case of failures.

This includes using technologies such as Spanning Tree Protocol (STP), EtherChannel, HSRP, VRRP or GLBP for link and device redundancy.

Using appropriate routing protocols at each layer to optimize routing performance and load balancing

Core Network Services

These are critical for the network to operate correctly. IP packets may flow in the network, but if these services don't reply or aren't configured correctly, users and devices won't be able to connect, and network applications won't be accessible.

They are:

- DNS
- DHCP
- NTP
- Authentication services

Design for Easy Management

- Good network designs are easy to maintain.

- When troubleshooting issues, IT teams should be able to identify the root cause quickly.

- Network devices and infrastructure should be labeled

Have inbuilt Fault Tolerance

- No matter how exceptional your network is, things will inevitably break.

- When they do, a fault-tolerant design can reduce disruptions and downtime.

- Have redundant components or paths in place so traffic can still flow if one part of the network fails.

  - Surge protectors

  - backup generators

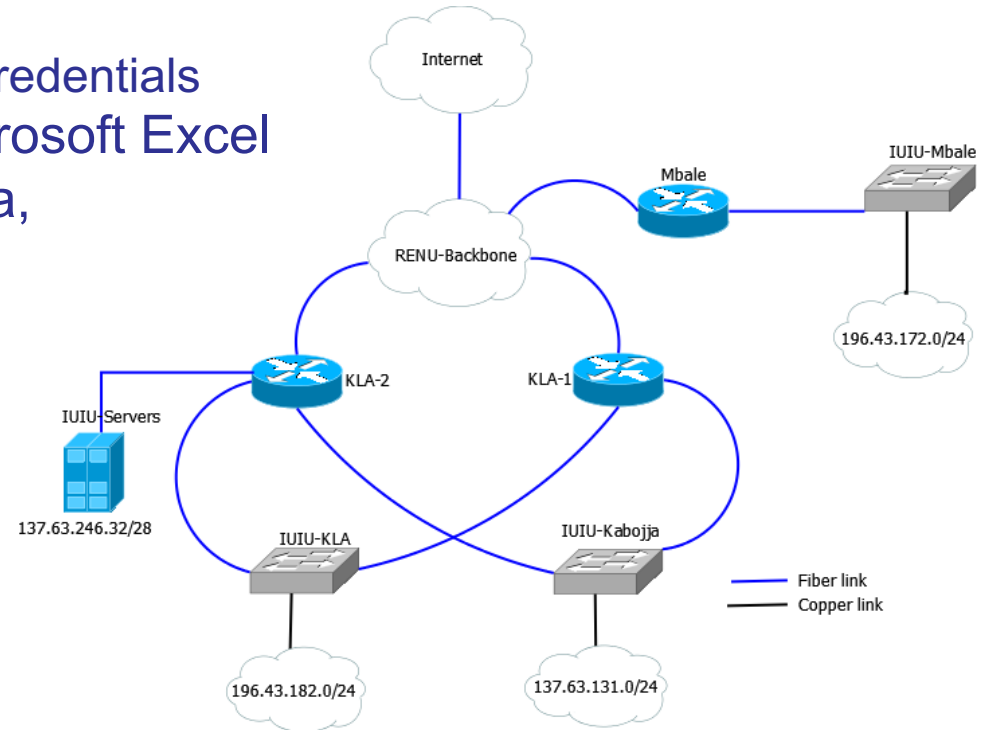 - fire-suppression systems

  - cloud-based data backups

Resource Allocation & Management

- IP Plan

- VLAN Plan

- Human resource
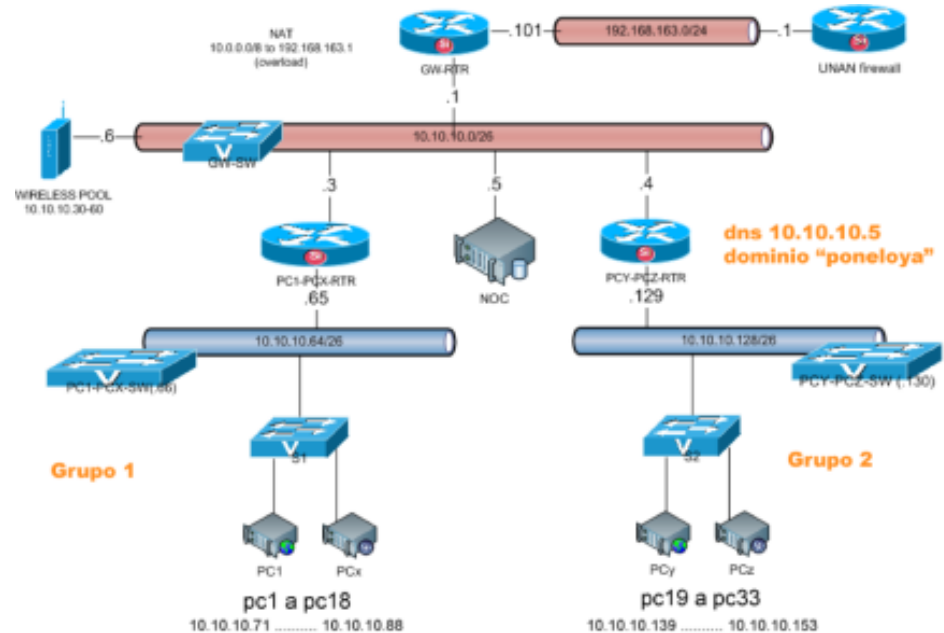
Document your network

- What to document?

  - Everything, devices, roles, credentials
- Basic network document; Microsoft Excel
- Network diagram, idraw.io, dia,

Monitor your network

- Monitoring – Check the status of a network
- Management – Processes for successfully operating a network
- Monitoring tools

Prioritize Security

- Design your network with security in mind.

- Incorporating devices and protocols that will protect your data from unauthorized access.

- Several steps you can take to increase security,

  - physical access to premises

  - installing firewalls

  - encrypting data

  - ensuring all devices are running the latest versions
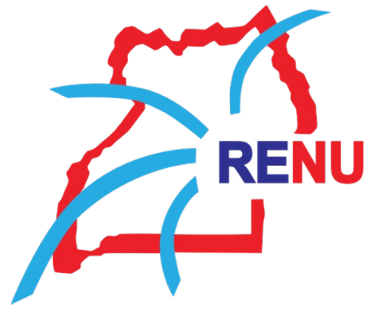
  - follow BYOD security best practices.

Summary

- R&E needs flexible and open networks

- Minimize number of network devices in any path

- Use the hub and spoke (star) configuration design pattern

- Segment your network with routers at the core/middle

- Provide services near the core

- Think carefully about where to firewall and where to NAT

- Your campus network must not be the bottleneck

- Make a plan for improvement

scenario

THE END

Thank you