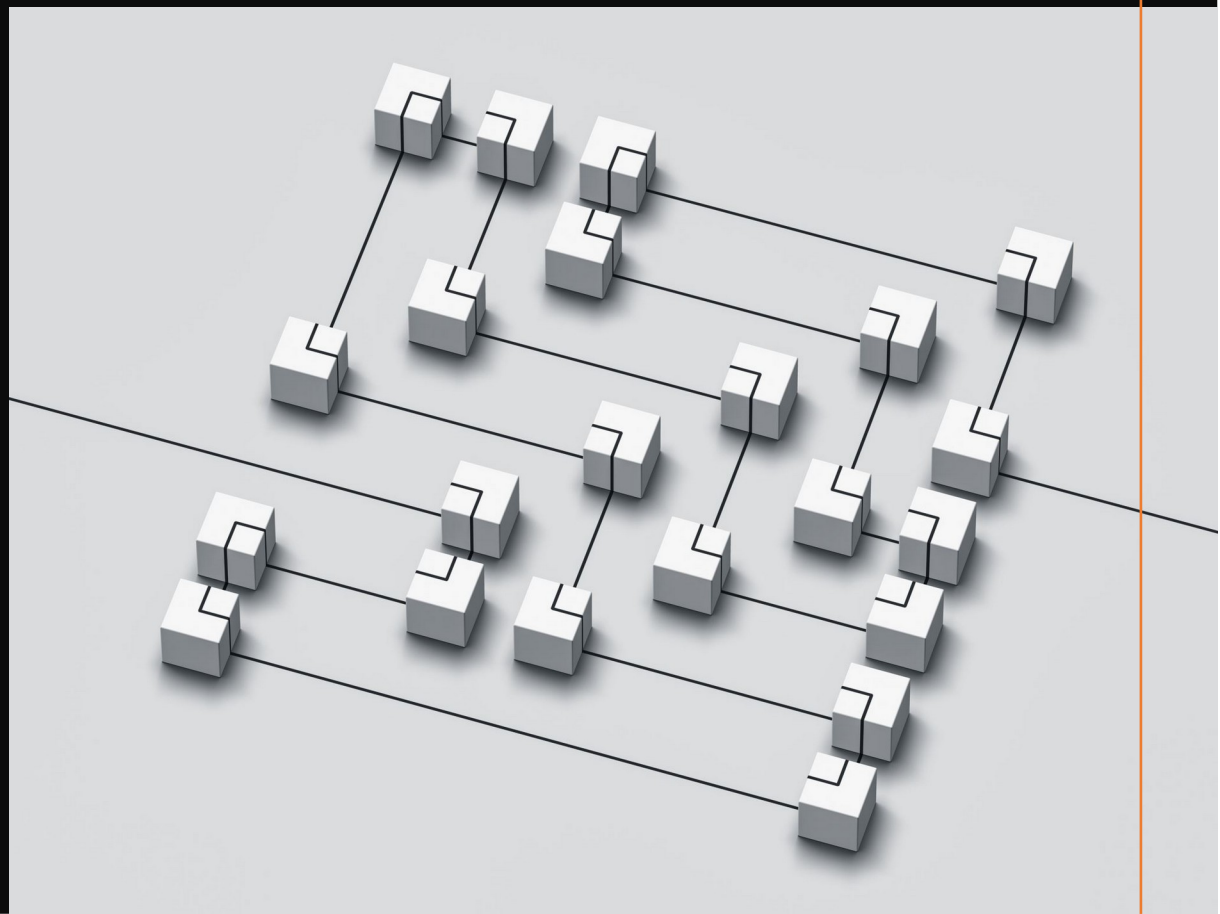
Scalable Campus Network Design & Operations - *Campus Network Design Principles*

Moses Ojiambo

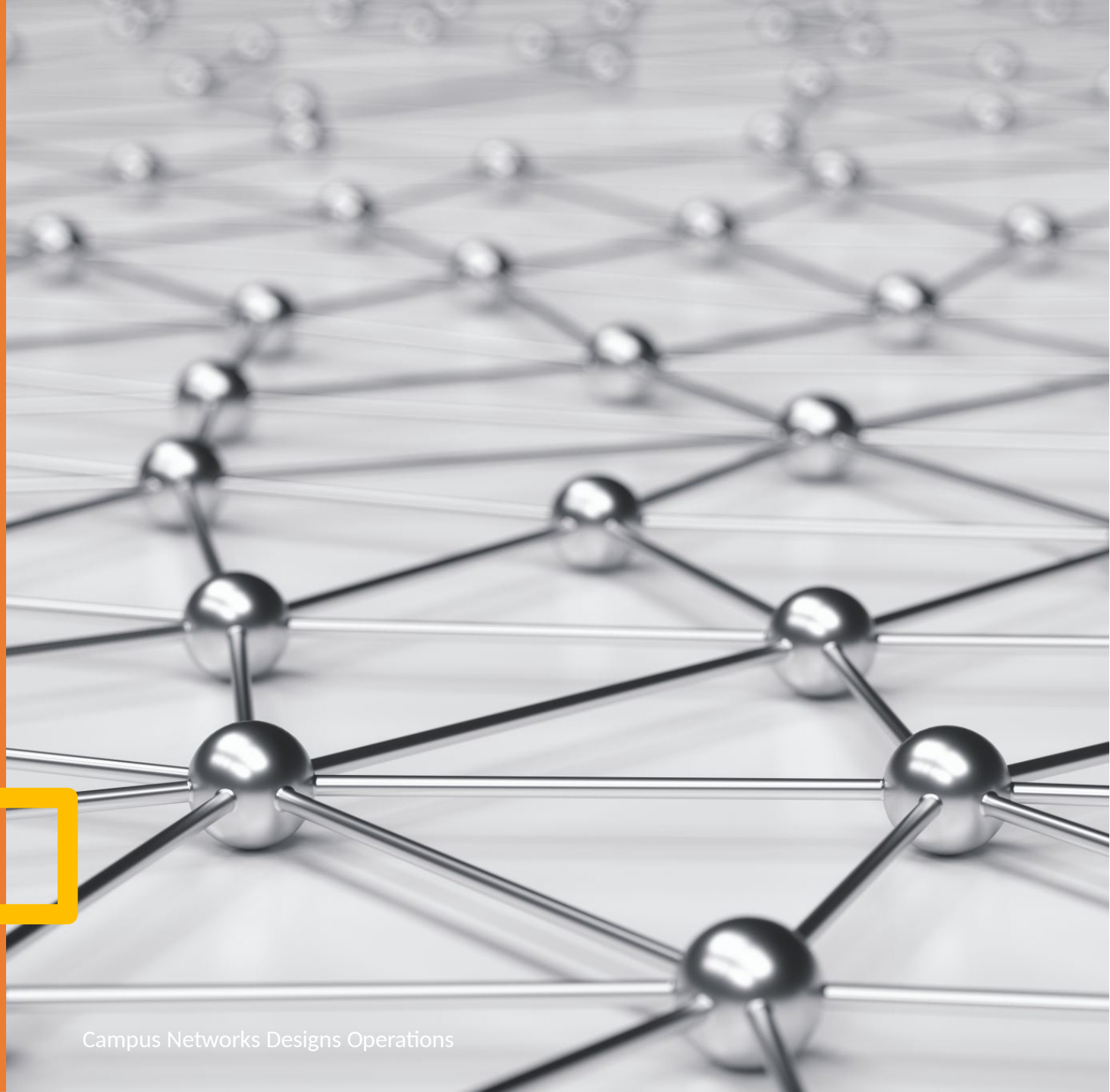
Transforming learning research and working environments with ICT

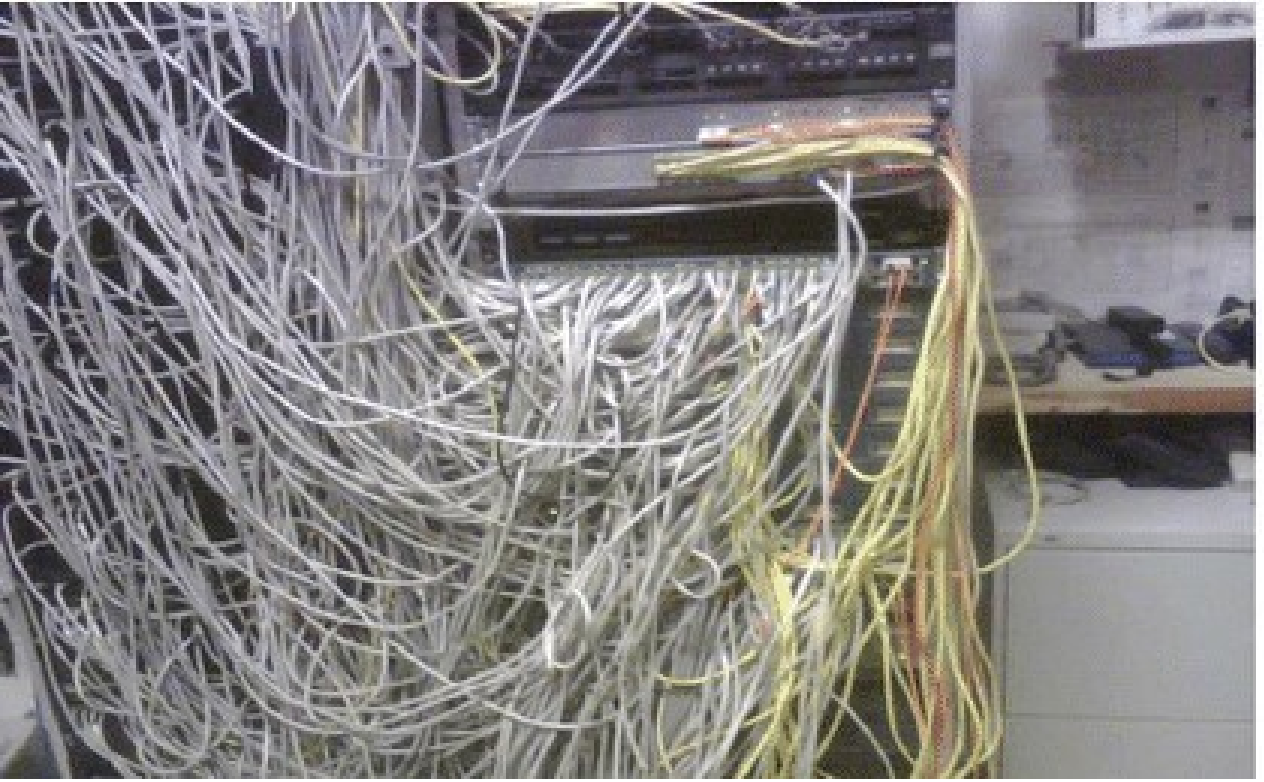
Agenda

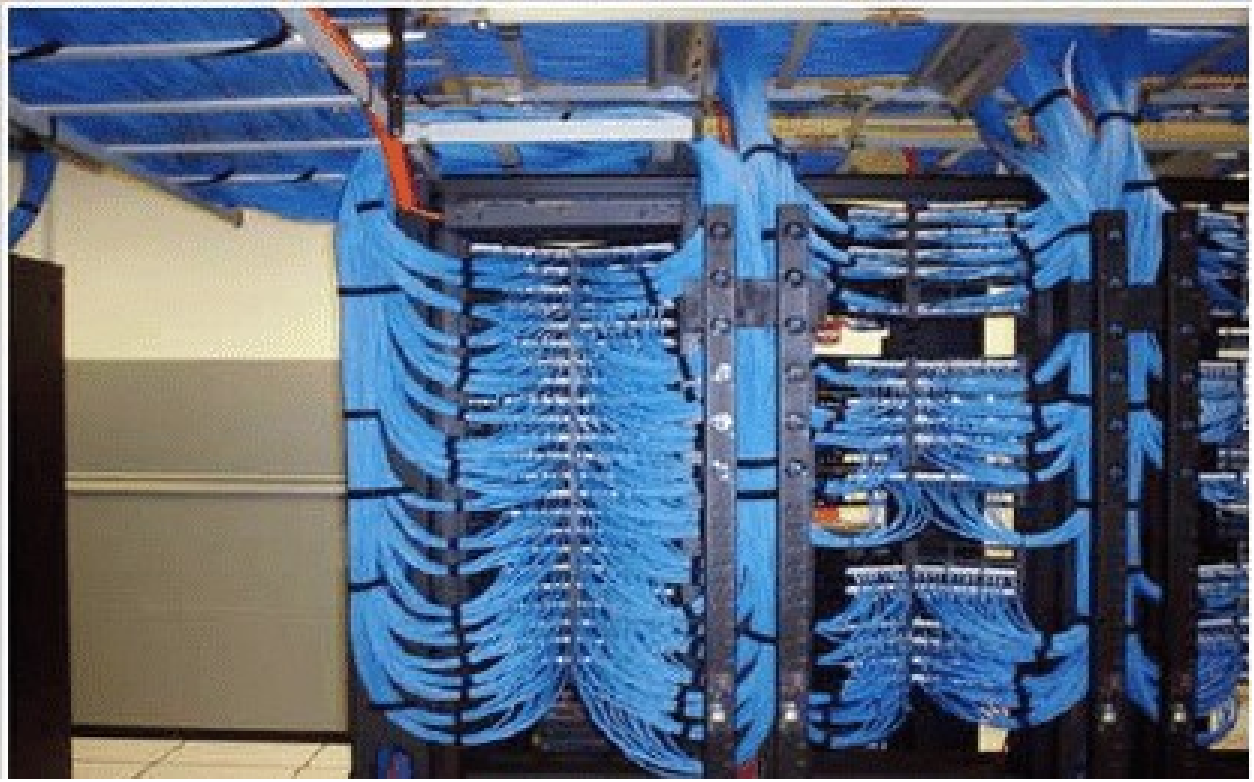
- Network Design Principles
- Layer 2 best practices (spanning, VLANs)
- IPv4 deployment best practices
- Campus Network Design Considerations



Network Design Principles







Campus Networks Challenges

- **Bad cabling/ unstructured** – No support for high bandwidth
- **Unmanaged devices** – “the enemy” – Cheap is expensive!
- **Daisy Chains** (Cascades) – violating STP device limit
- **NO Monitoring (Network Management Systems)**
- **Frequent Power outages**

Campus Networks Design Consideration

1. **Capacity** – How many devices are accessing the network?

- Which Services are supported? (Data, Voice, Video)?

2. **Coverage** – Extend coverage to critical areas (gradual growth – small incremental changes)

3. **Security** – Protect systems and applications

4. **Density** – Concurrent connections (auditorium?)

5. **Cost** – Total Cost of Ownership (TCO) including hardware refresh

6. **Performance monitoring** – Proactive monitoring for optimal operation

Step-by-Step Best Design Logical Sequence

Spanning Tree (RSTP)

Minimize number of network switches in any single path (chain) - STP limit is 7 nodes

Network Topology

Use the hub and spoke (STAR) configuration design. Eliminate points of failure

VLAN Implementation

Segment your networks using VLANs and remember to route at the core

Server Placement

Provide Services near the core

Firewall Placement

Think Carefully about where to firewall and where to NAT

Core Network Design (Server ~~room/Data Centre~~)

Reliability is the GOAT! – Remember the whole network relies on the core

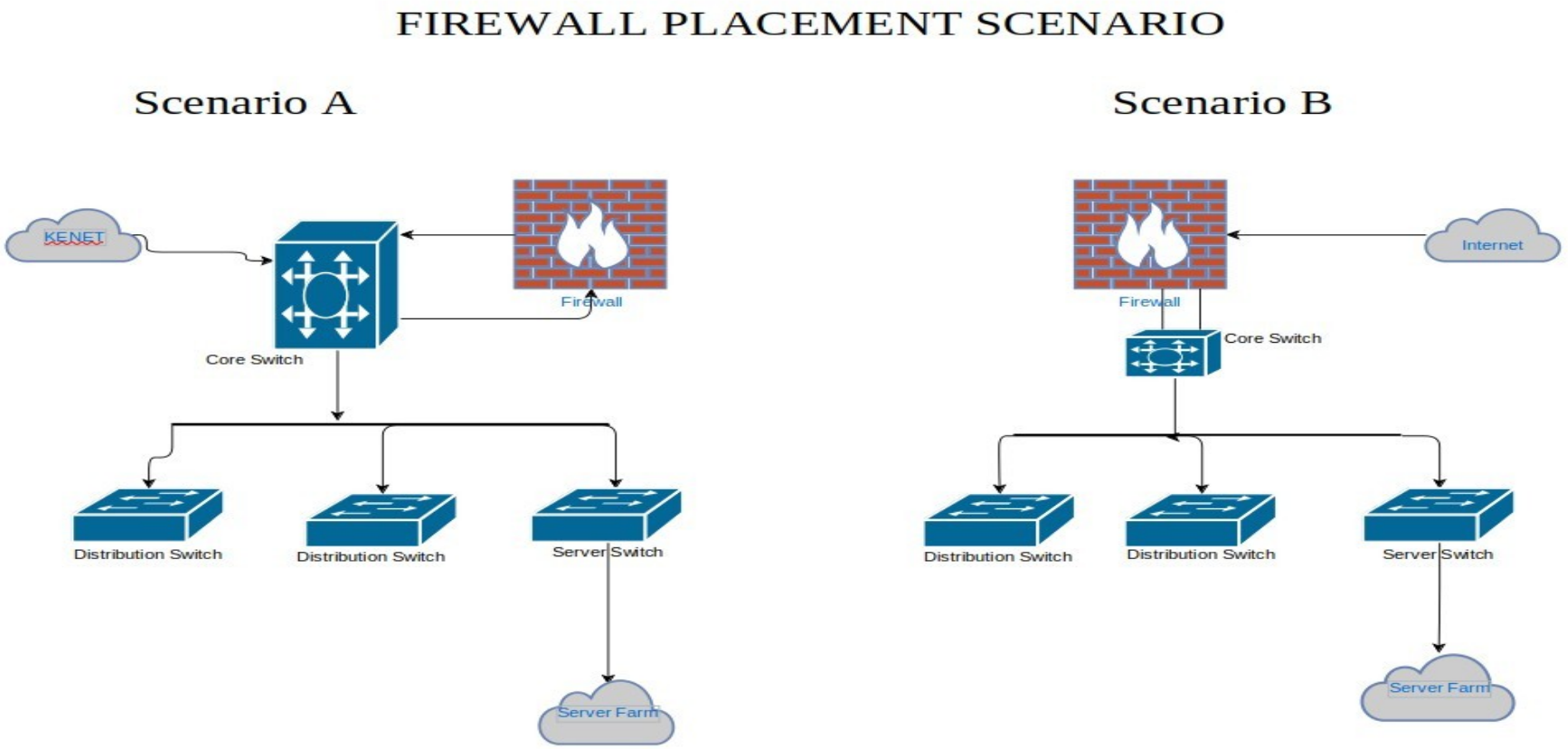
MUST Haves…

1. **Stable Electrical Power Supply** – AVR for voltage stabilization
2. **UPS backup** (*redundant UPSes as your network evolves*)
3. **Generator / Solar backup**
4. **Proper grounding /earthing**

5. Lightning arrestor for lightning prone areas

6. **Reliable air conditioning –** repair faulty ACs
7. **Network/ Server Cabinets**
8. **Fire Suppression –** minimum hand-held fire extinguisher

Where to place the [illegible]



Where to place Servers

- Servers should be placed at your core location where there is good power and air conditioning
- Put different classes of servers on different subnets:
  - Sensitive systems (payroll, financial systems, procurement systems (ERP) etc)
  - Network services (DHCP, DNS, NTP, NMS, Authentication services – Radius, LDAP, active directory, TACACs+ etc)
  - Student systems

Migrating a Campus Network: Flat to Segmented

A. *IPv4 Subnetting (CIDR application) – VLAN Subnets*
B. *Spanning Tree Protocol (RSTP)*
C. *Network Security (Firewall)*
D. *Network Topology (Star – Hierarchical/Extended)*
E. *Core Network Services*

1. *DHCP*
2. *DNS*
3. *NTP*
4. *Authentication services*

IPv4 Subnetting Example

Proposed Institution XYZ VLANs & IPv4 Address Subnets Scheme

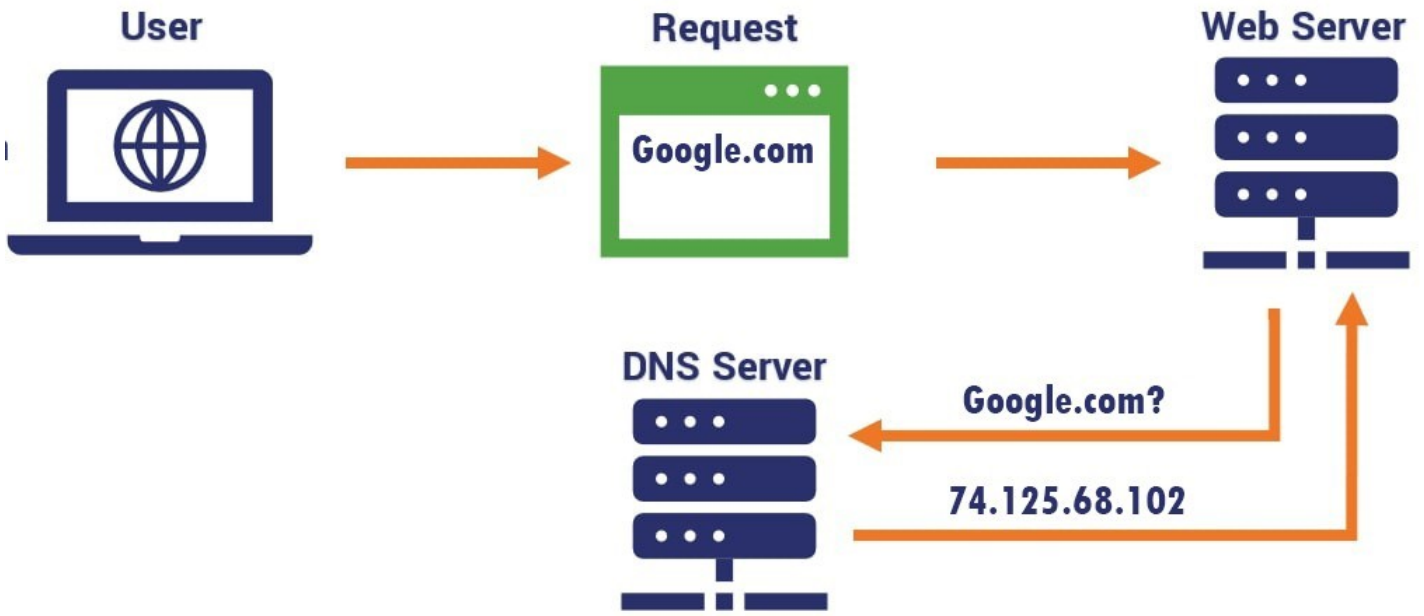
Item	VLAN	VLAN Name	IPv4 Subnet	Subnet Mask	Gateway	Usable Addresse	1st Usable IPv4 Address	Last Usable IPv4 address	Reserved Addresses	IP Assignment
	100	PUBLIC	41.89.xx.0/24	255.255.255.0	41.89.xx.1	254	41.89.xx.2	41.89.xx.254	41.89.xx.1	Static
1	CCTV	CCTV	172.16.0.0/23	255.255.254.0	172.16.1.254	510	172.16.0.1	172.16.1.254	172.16.0.0 – 172.16.1.254	Static
2	2	Device_Management	172.16.32.0/21	255.255.255.0	172.16.39.254	2046	172.16.32.1	172.16.39.254	172.16.11.244 – 172.16.11.254	DHCP
3	3	Voice	172.16.40.0/23	255.255.254.0	172.16.41.254	510	172.16.40.1	172.16.41.254	172.16.41.154 – 172.16.41.254	DHCP
4	4	Admin	172.16.42.0/24	255.255.255.0	172.16.42.254	254	172.16.42.1	172.16.42.254	172.16.42.244 – 172.16.42.254	DHCP
5	5	Library	172.16.43.0/24	255.255.255.0	172.16.43.254	254	172.16.43.1	172.16.43.254	172.16.43.244 – 172.16.43.254	DHCP
6	6	Digital_Library	172.16.44.0/24	255.255.255.0	172.16.44.254	254	172.16.44.1	172.16.44.254	172.16.44.244 – 172.16.44.254	DHCP
7	7	Finance	172.16.45.0/24	255.255.255.0	172.16.45.254	254	172.16.45.1	172.16.45.254	172.16.45.244 – 172.16.45.254	DHCP
8	8	Exams	172.16.46.0/24	255.255.255.0	172.16.46.254	254	172.16.46.1	172.16.46.254	172.16.46.244 – 172.16.46.254	DHCP
9	9	ICT	172.16.47.0/24	255.255.255.0	172.16.47.254	254	172.16.47.1	172.16.47.254	172.16.47.244 – 172.16.47.254	DHCP

Core Network Services: DHCP

Core Network Services: DHCP

- -It's a good idea to reduce the lease time in advance of renumbering
- -Configure DHCP relay to minimize broadcast storm
- Place DHCP servers near the core
- Configure DHCP relaying on each subnet facing interfaces
- Broadcast DHCP messages from clients are relayed to DHCP servers in the core
- To avoid rogue DHCP servers, consider setting up DHCP snooping
- – Blocks DHCP replies from non authorized DHCP servers

Core Network Services: DNS



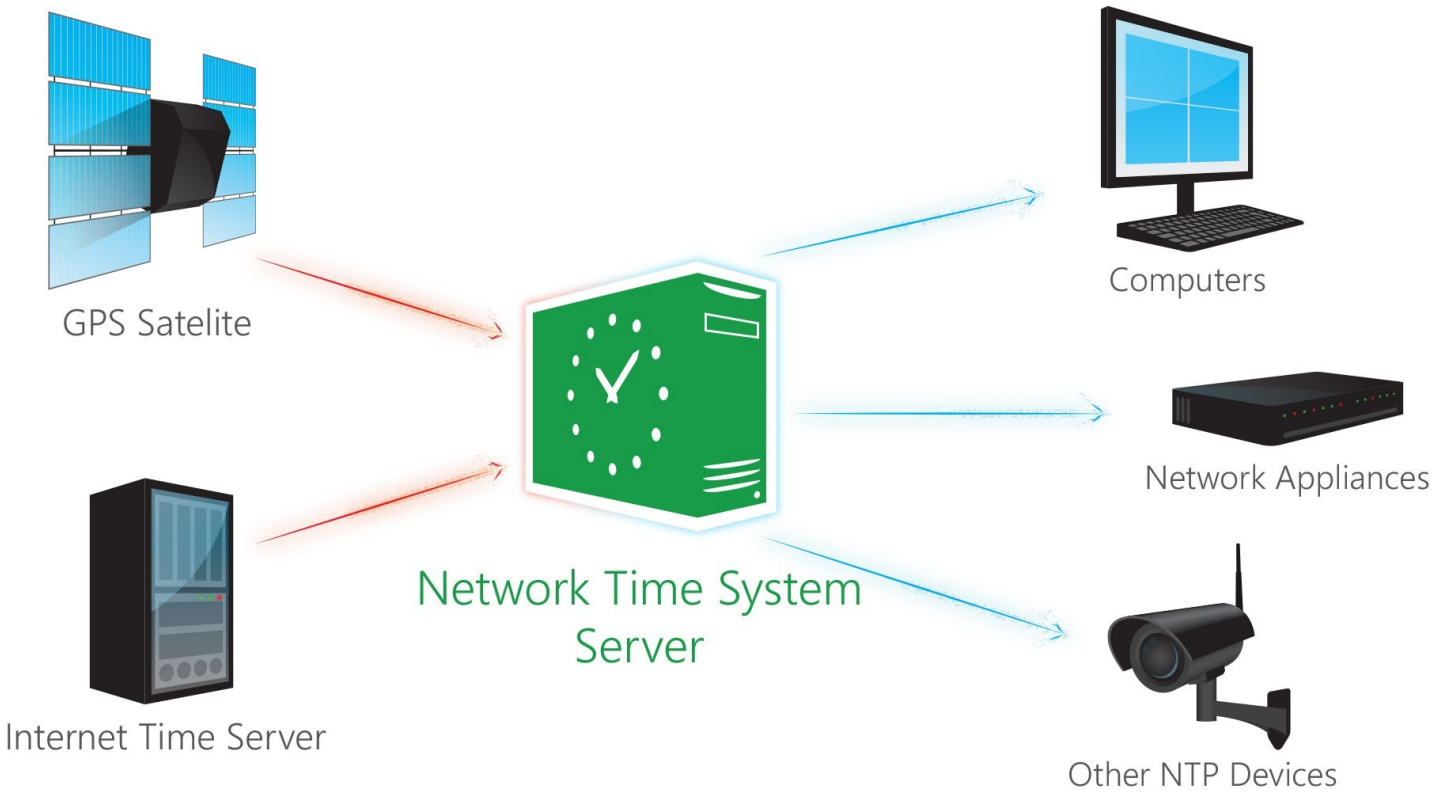
Core Network Services: DNS

Recommendation – Setup a Caching Name Server (Resolver) on Campus

Campus networks must offer reliable & fast (low latency) DNS service

– Have on-campus, fast caching resolvers

Core Network Services: NTP



Core Network Services: NTP

Accurate time keeping is critical for the network to function properly, and to maintain synchronized logs across devices

– Use consistent timezones: either UTC or your local time zone

Core Network Services: Authentication Services

Many possibilities, you might have:

- User database: Active Directory, FreeIPA, LDAP, SQL…
- RADIUS server (802.1x wireless authentication)
- Captive portal

Q&A

Thank You

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100,
Nairobi. 0732 150 500 / 0703