kenet
Kenya Education Network

Campus Network Best Practice

BMO Training 2013

Kennedy Aseda
Senior Network Engineer

Overview

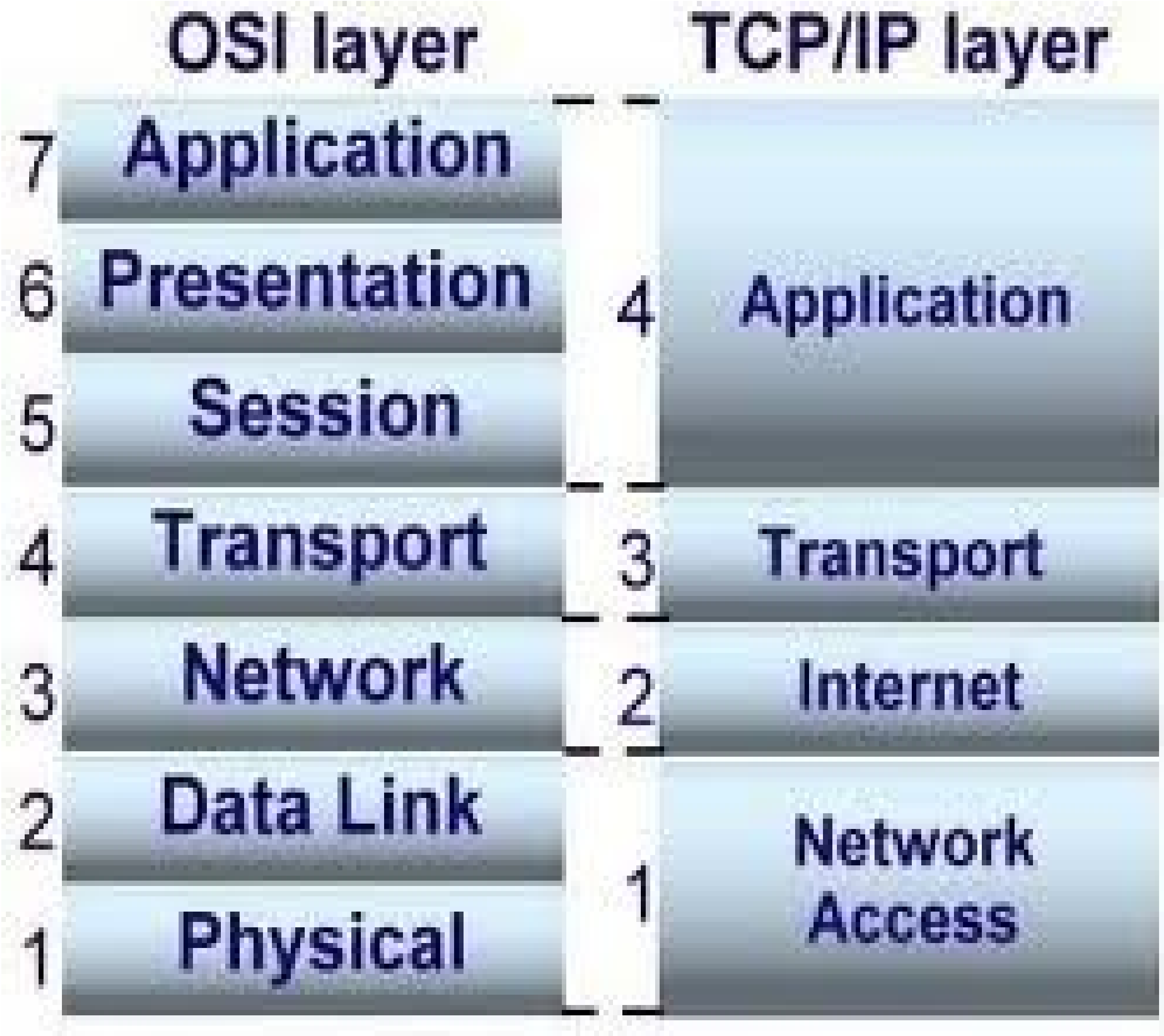
- TCP/IP Protocol Stack
- Layer 1
- Layer 2
- Layer 3
- Layers 4-7
- Monitoring & Documentation
- Q&A

The Bottom Line

- Our Goal?
  - Ensure KENET members have capacity to support R&E
  - KENET exists because its members exist
  - No campus networks, No KENET
- KENET the REN
  - Affordable connectivity
  - Power of collective bargaining
  - Public IP Space – For Members
  - Increase student/PC ratio – E-readiness Survey
  - Provide the human networking
  - Etc

kenet
Kenya Education Network

OSI & TCP/IP Protocol Stack



	OSI layer		TCP/IP layer
7	Application	4	Application
6	Presentation		
5	Session		
4	Transport	3	Transport
3	Network	2	Internet
2	Data Link	1	Network Access
1	Physical		

Layered Model - Logical

- A good network design is modular and hierarchical, with a clear separation of functions:

Core:

Resilient, few changes, few features, high bandwidth, CPU power

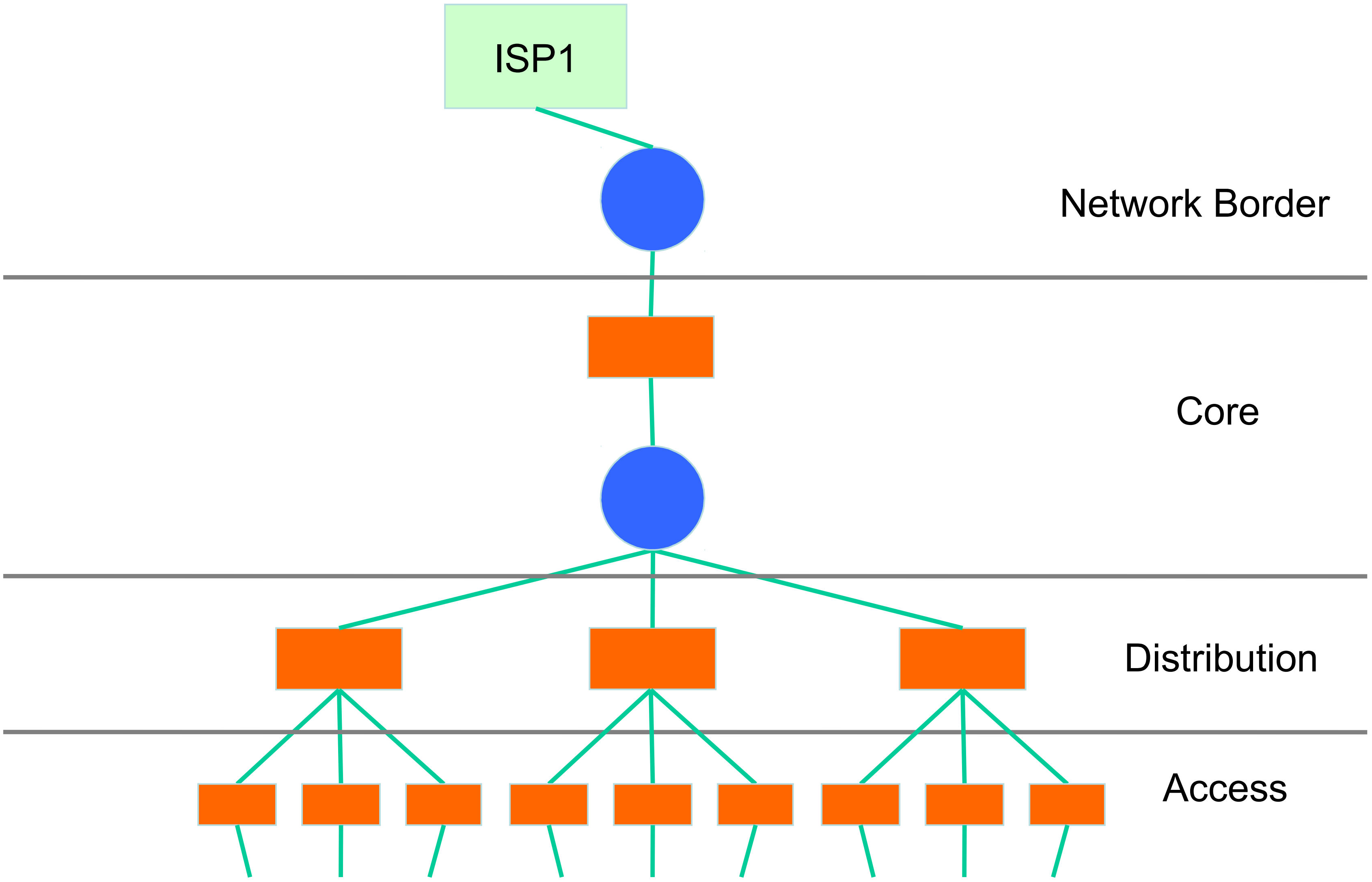
Distribution:

Aggregation, redundancy

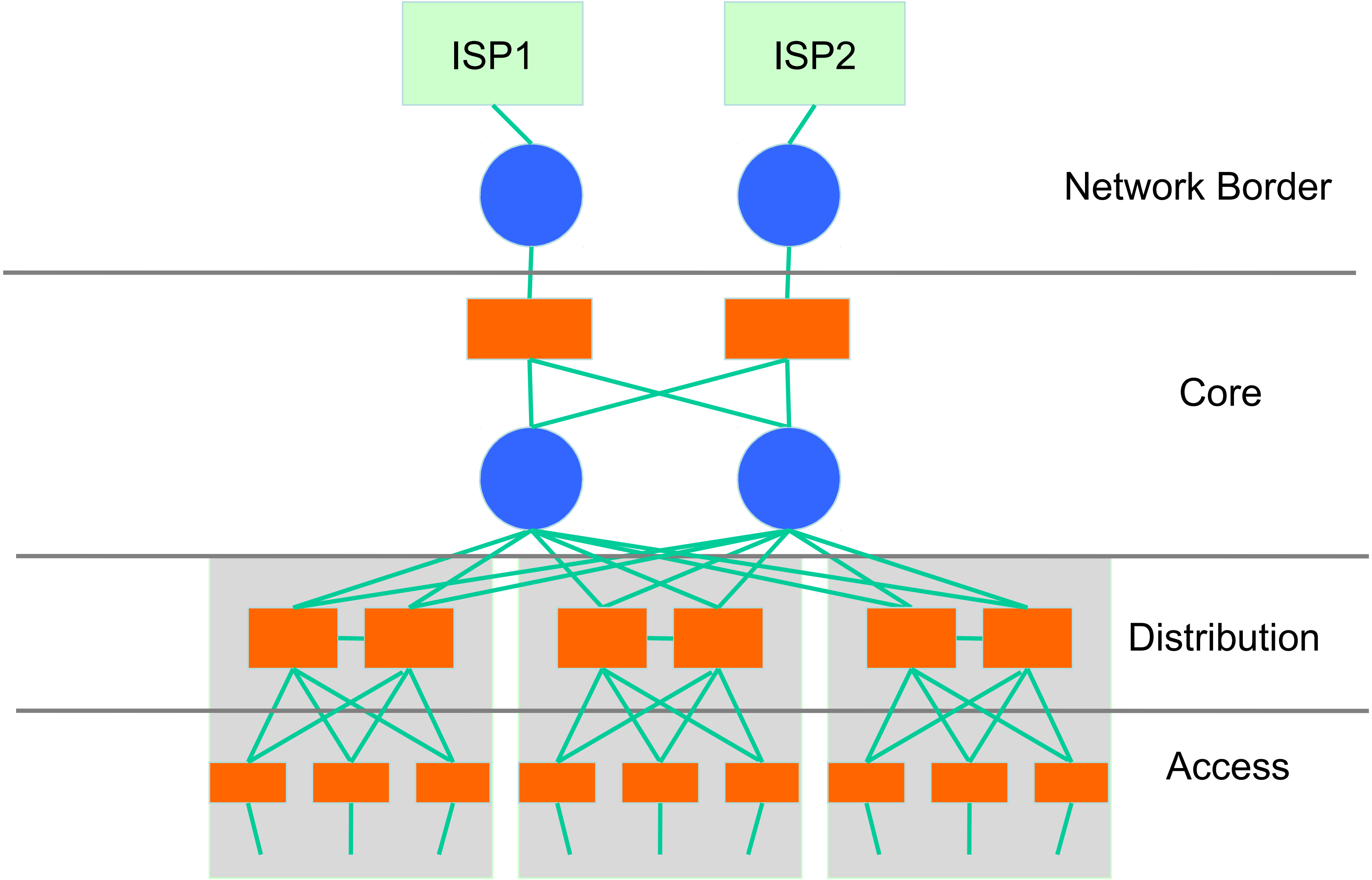
Access:

Port density, affordability, security features, many adds, moves and changes

Campus Network Design - Simple



Campus Network Design - Redundant



kenet
Kenya Education Network

Layer 1: Physical Network & Environment

- Cabling/Medium Best Practices
  - Copper
    - Connect end users to the access network
  - Fiber
    - Connect buildings to the core
    - Single Mode/Multimode?
    - Star Topology
    - Need more out of fewer pairs?
    - WDM/Coloured interface devices
  - Wireless
    - Complement to cable/not a replacement

Fiber Optic Topology

Fiber Types

Multi mode: don’t bother if run is over 200M

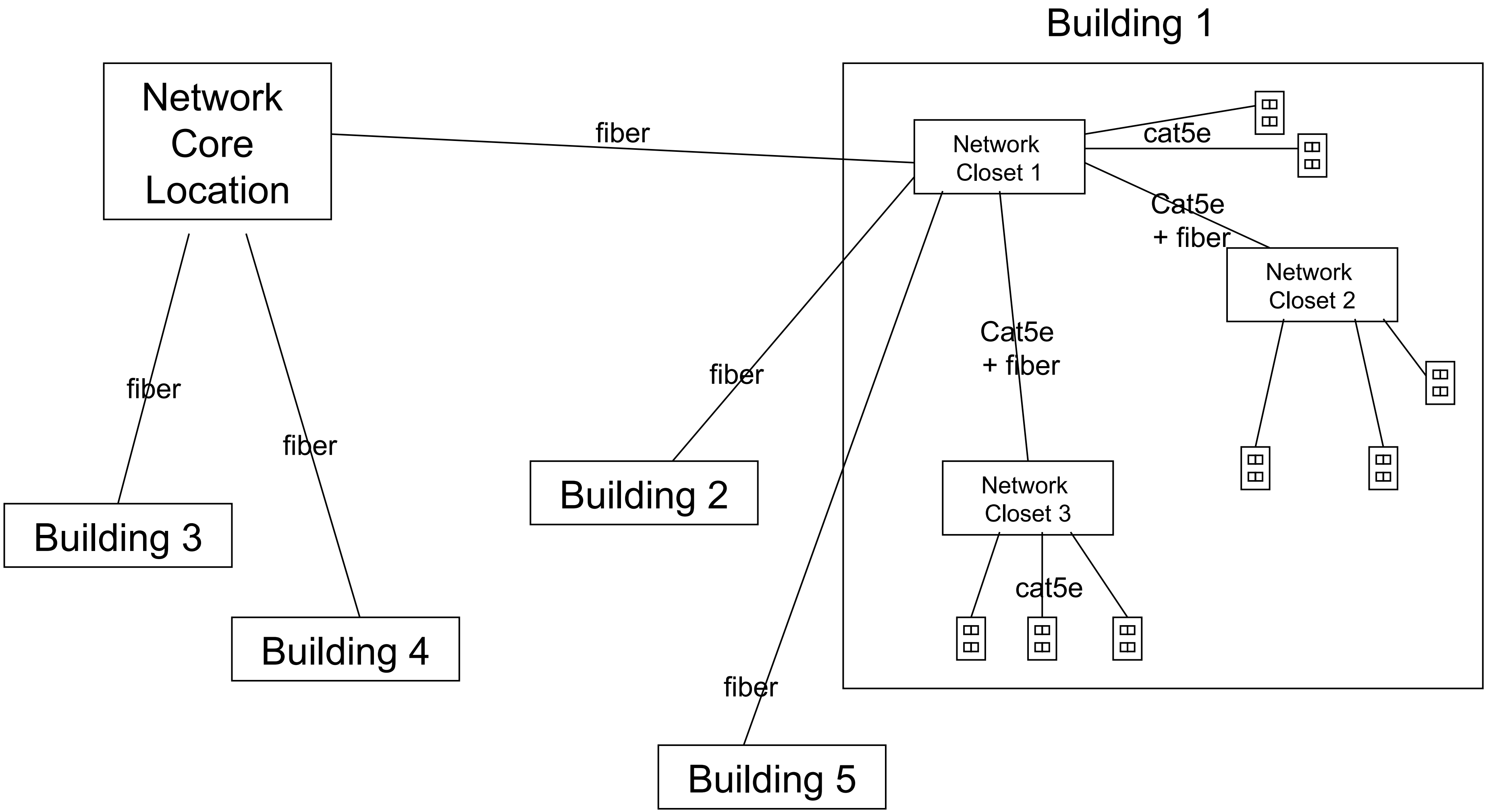
Single mode: use fiber optimized for 1310/1550nm

Run in star configuration from core network location to individual buildings

Also run in star configuration inside of buildings from main phone closet to other closets

To reduce costs, can run large fiber cable from core to some remote location, then smaller cables from there to surrounding buildings

Putting it all Together

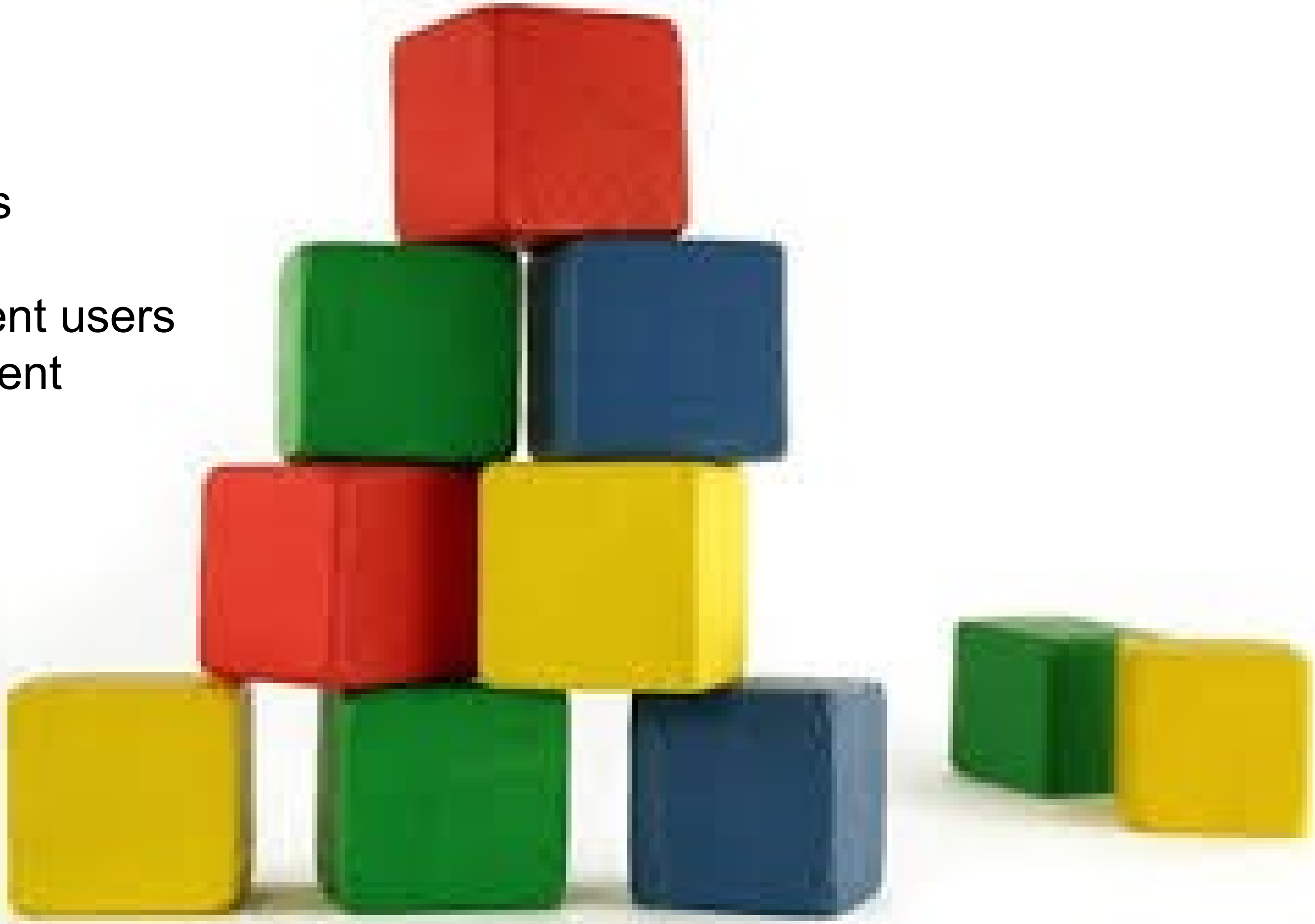


Layer 1: Physical Network & Environment

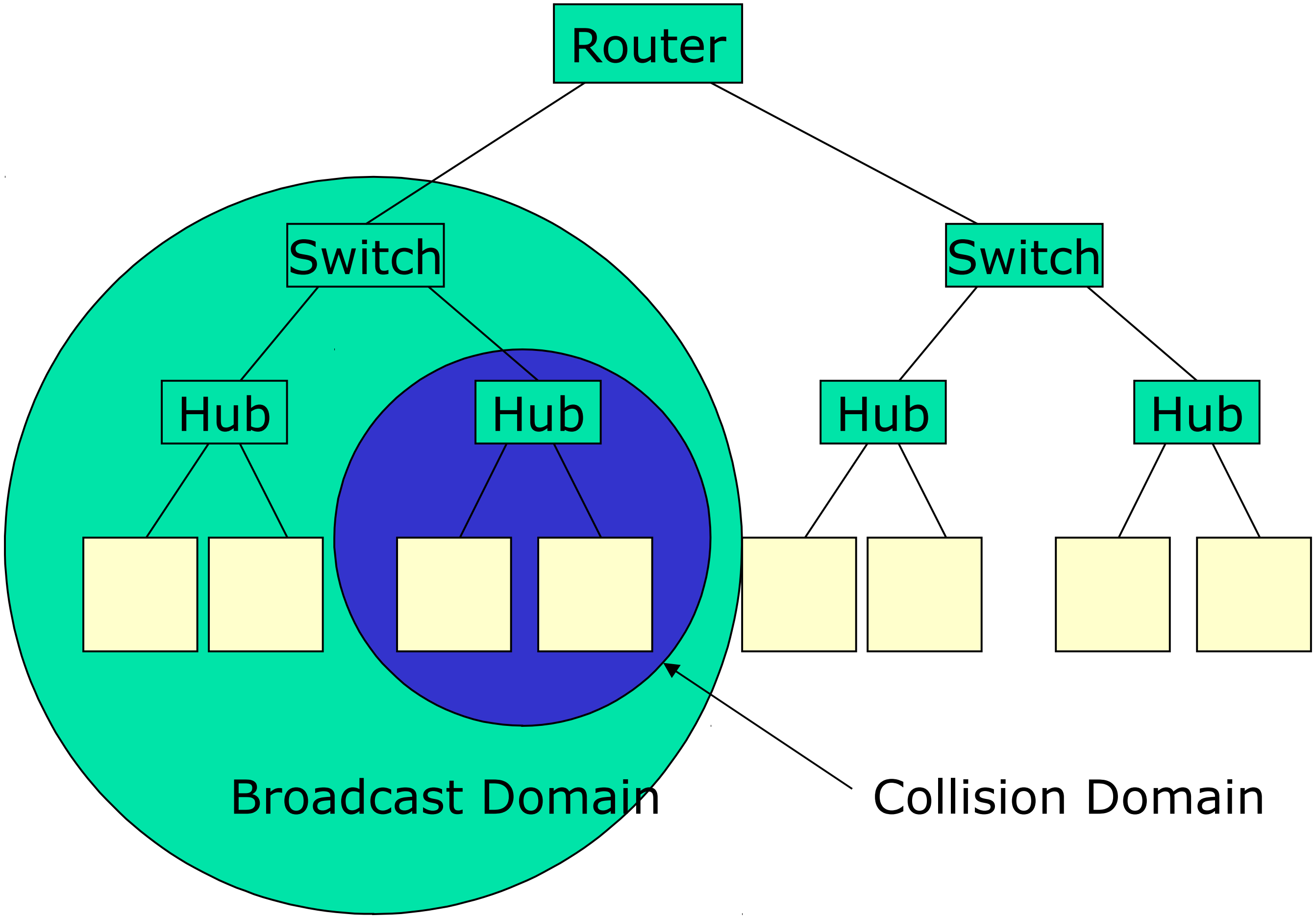
- Power
  - UPS Power
  - Generator
- Air Conditioning
- Fire Suppression
- Cabinets
  - Cable Management
  - Earthing/Grounding

Layer 2: Network Devices

- Network Switches
  - Core
  - Distribution
  - Access
- VLANs
  - The Layer 2 Problem
    - Collision Domains
    - Broadcast Domains
    - Switching Loops
  - Use VLANs to segment users
    - Network Management
    - Servers
    - Departments
    - LABs
    - Private VLANs
  - Security
    - VLAN Access Lists
    - Port Access List



Traffic Domains



Router

Switch

Switch

Hub

Hub

Hub

Hub

Broadcast Domain

Collision Domain

Traffic Domains

Try to eliminate collision domains

Get rid of hubs!

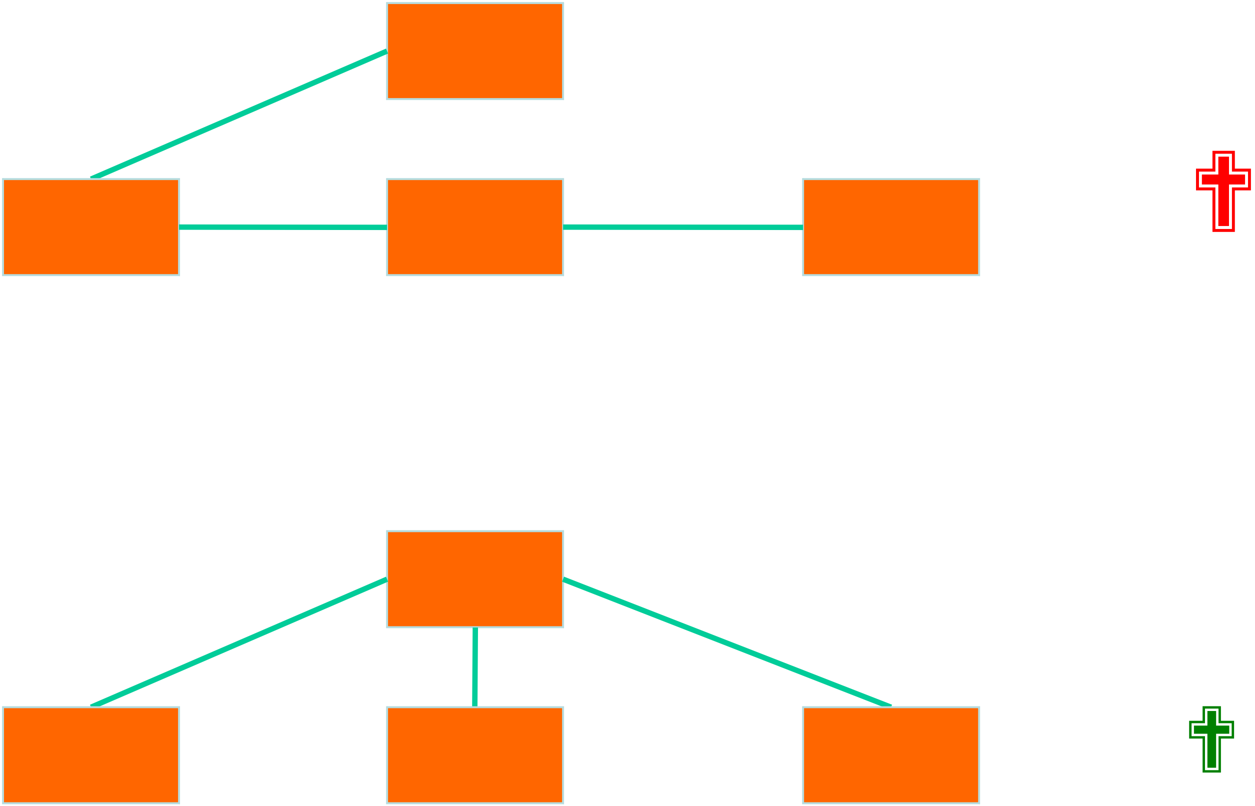
Try to keep your broadcast domain limited to no more than 250 simultaneously connected hosts

Segment your network using routers

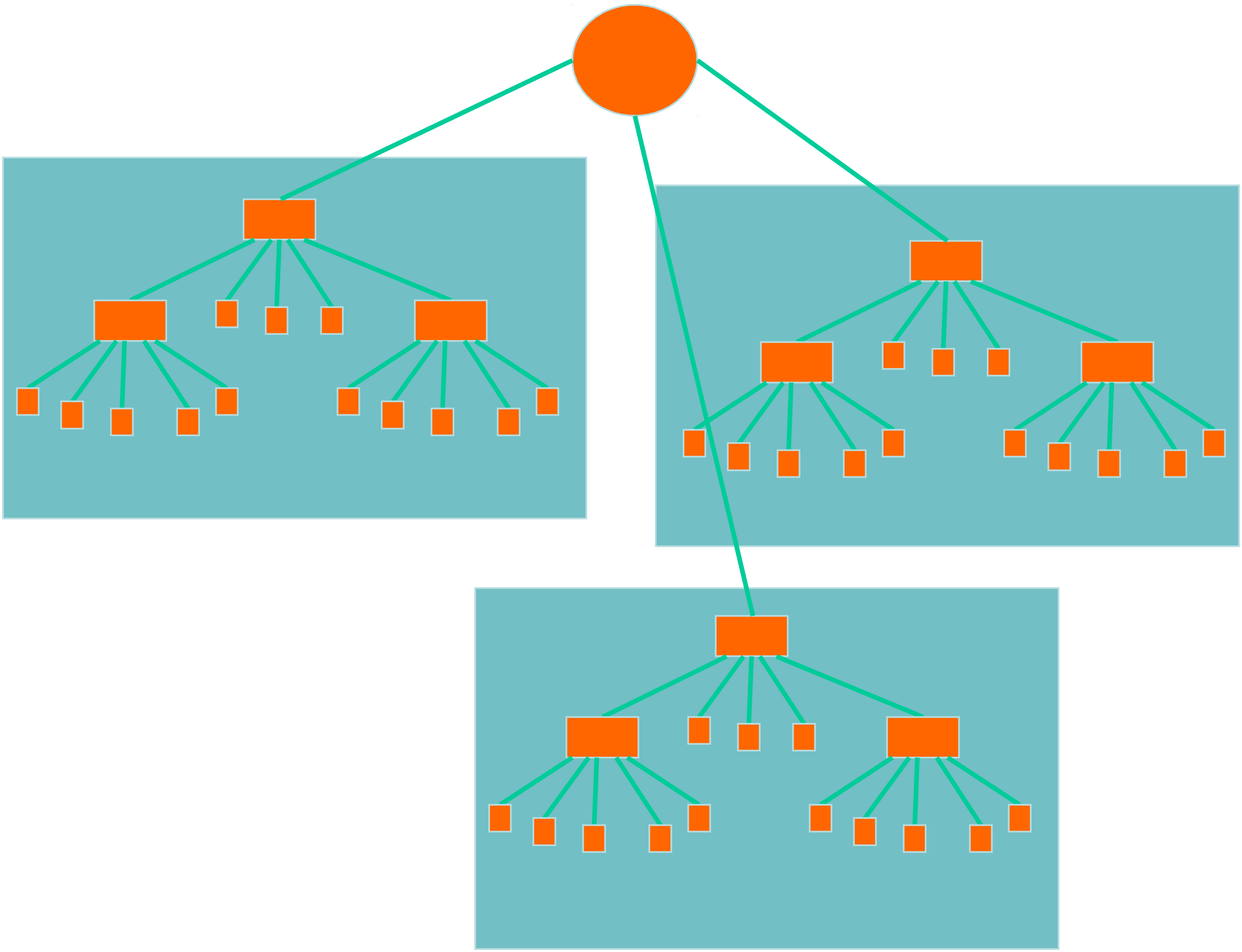
kenet

Kenya Education Network

Minimize Path Between Elements



Connect buildings hierarchically



Layer 3: Network Routers/Gateways

- IP Addressing
  - DHCP Server
- IP Firewall - Close unused IPs
  - Host Based Firewall
  - Network Firewall
- NATing?
  - Used to reduce public IP requirements
  - Makes user identification difficult
  - Breaks SIP, Video Conferencing

Layer 4-7: Services & Security

- Web Caching/Acceleration
  - Squid
- Security - Close unused services
  - Firewall (Layer 4-7)
  - IDS
  - IPS
- Rules of Access
  - NAC – Packetfence
- Helpers
  - DNS

Network Expansion

- Ensure upcoming buildings have ICT infrastructure built in
  - Reduces pressure on ICT to invest in new buildings
  - Ensures ICT budget is not touched by expansions
- Ensure your institution has a master plan
  - Helps to plan fiber routes, etc

kenet
Kenya Education Network

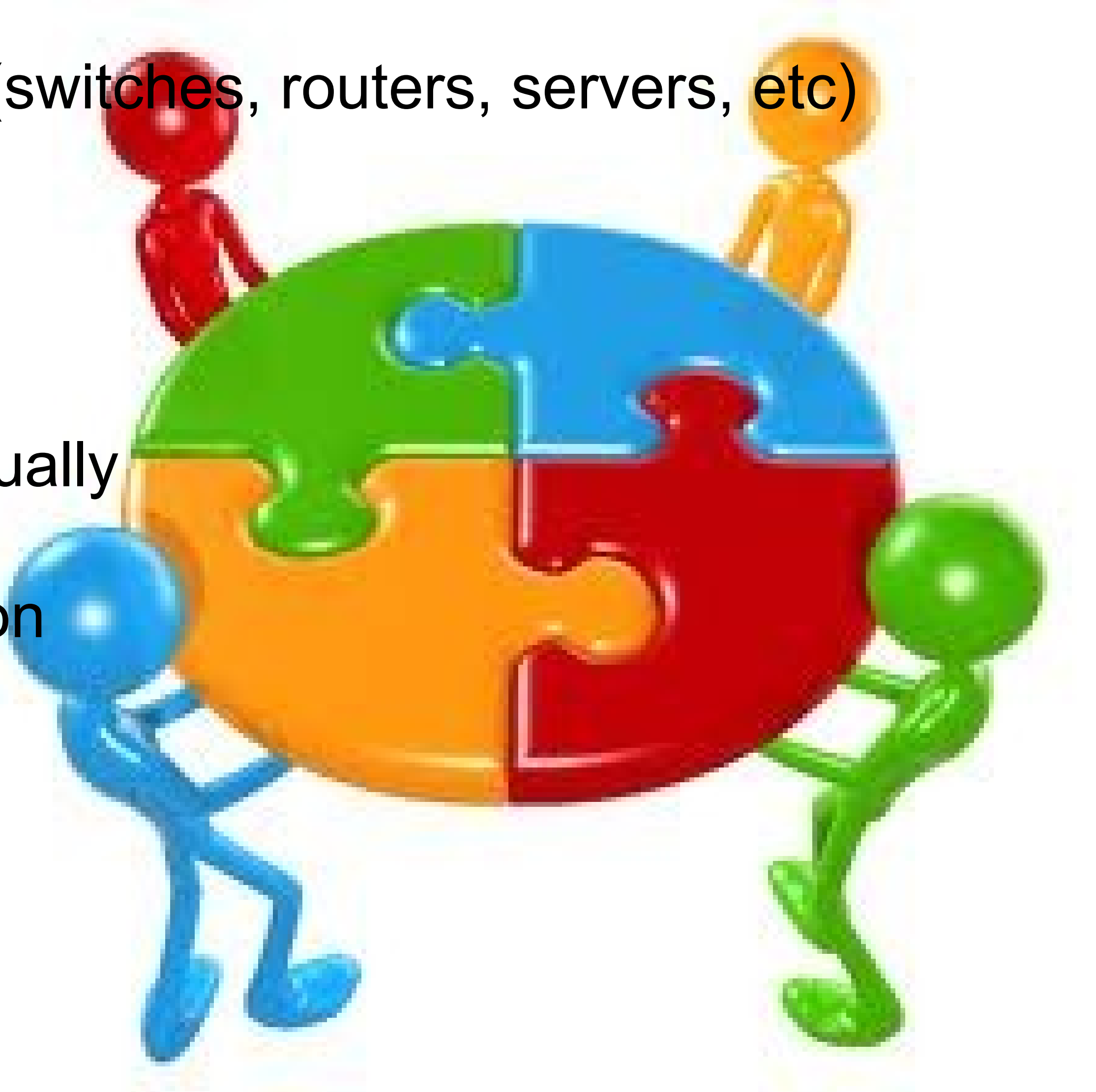
Routine Checks/Monitoring

- Physical Checks
  - Routine physical checks helps identify if AC is leaking, etc
  - Ensure users log their visits
- Automated Tools
  - Availability
  - Traffic Utilization
  - Network Latency
  - Device Logs
- Routine Maintenance
  - UPS, Genset, Fire fighting, Air Conditioning, Switches, Servers, etc

kenet
Kenya Education Network

Documentation

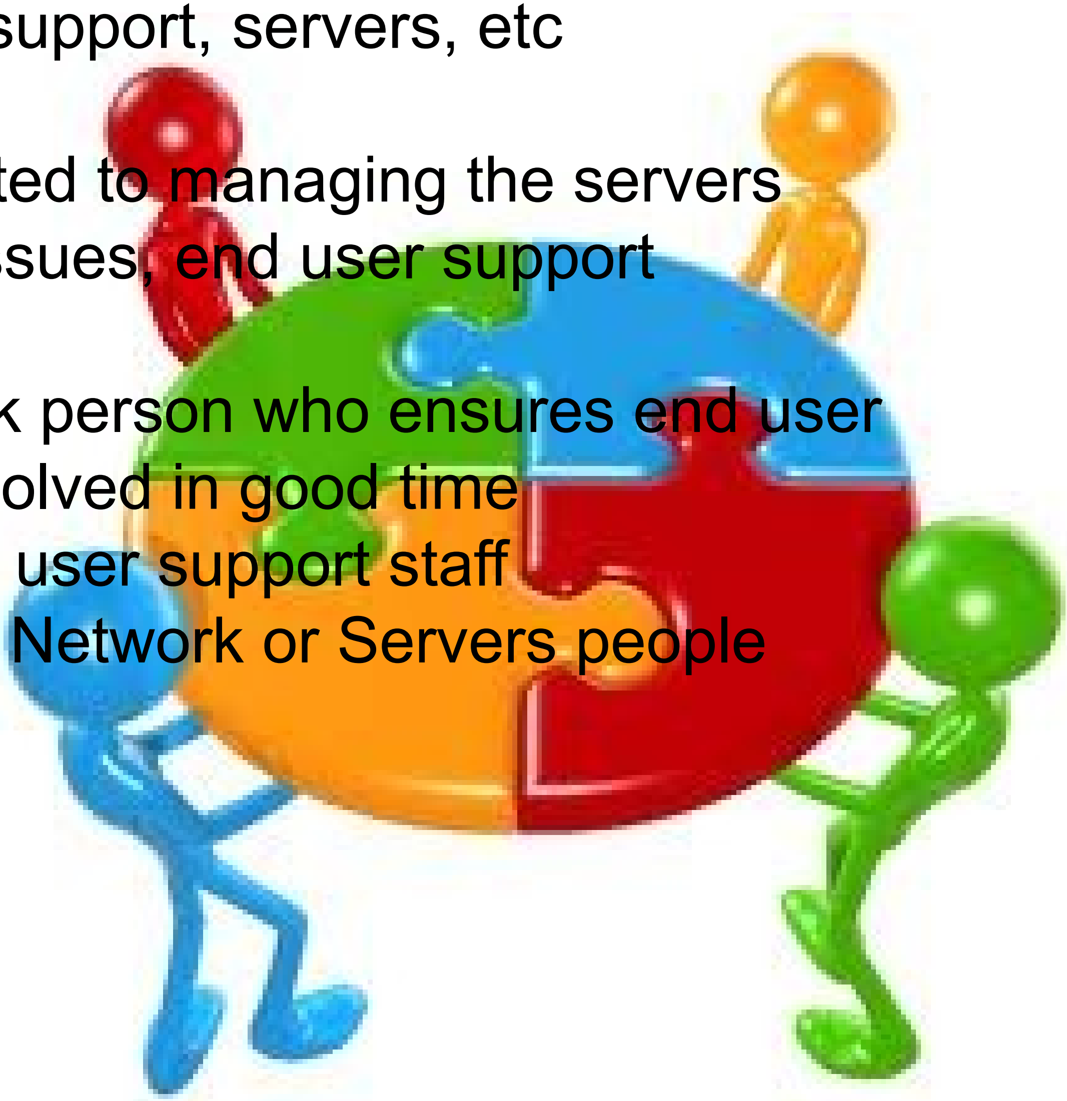
- Labeling
  - Label cables
  - Label all racks/cabinets
  - Label all network devices (switches, routers, servers, etc)
- Device Documentation
  - Keep physical inventory
  - Use automated tools
- Configuration Backup
  - Back up configuration manually
  - Use automated tools
- IP Addressing Documentation



kenet
Kenya Education Network

Personnel

- Campus Network
  - At least one person dedicated to the network
  - Does not handle end user support, servers, etc
- Network Servers
  - At least one person dedicated to managing the servers
  - Does not handle network issues, end user support
- User Support
  - Have a dedicated help desk person who ensures end user requests/complains are resolved in good time
  - Should have a team of end user support staff
  - Escalate difficult probles to Network or Servers people



kenet
Kenya Education Network

Q
&
A