University of Colorado **Boulder**

Network Management and Automation

Network Design

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

- **Network Design Lab**
  - Teams posted
  - Lab requirements posted
    - ***Two Weeks***
      - Week 1 – Network Design (Report & Presentation)
        - » Tuesday & Thursday–*Presentations (15 min)
      - Week 2 – Proof of Concept (Report & Presentation)
        - » Tuesday & Thursday–*Presentations (15 min)

- **Today's lecture**
  - Entire Network Design semester course in one lecture
  - Pre-sales & Systems Engineering roles
  - How to communicate technical information (sales)
  - CCDA/CCDP
  - Security
  - Think to yourself
    - ***Consulting vs Ownership***

IP Network Design

- **A competent network design is the foundation upon which all successful network implementations are built**
  - Fundamental principles
  - IP addressing
  - Designing the LAN
  - Designing the WAN

Organization and Technical Constraints

- **Organizational**
  - Budget
  - Personnel
  - Policy
  - Scheduling

- **Technical**
  - Existing equipment
  - Bandwidth availability
  - Application compatibility

Lifecycles

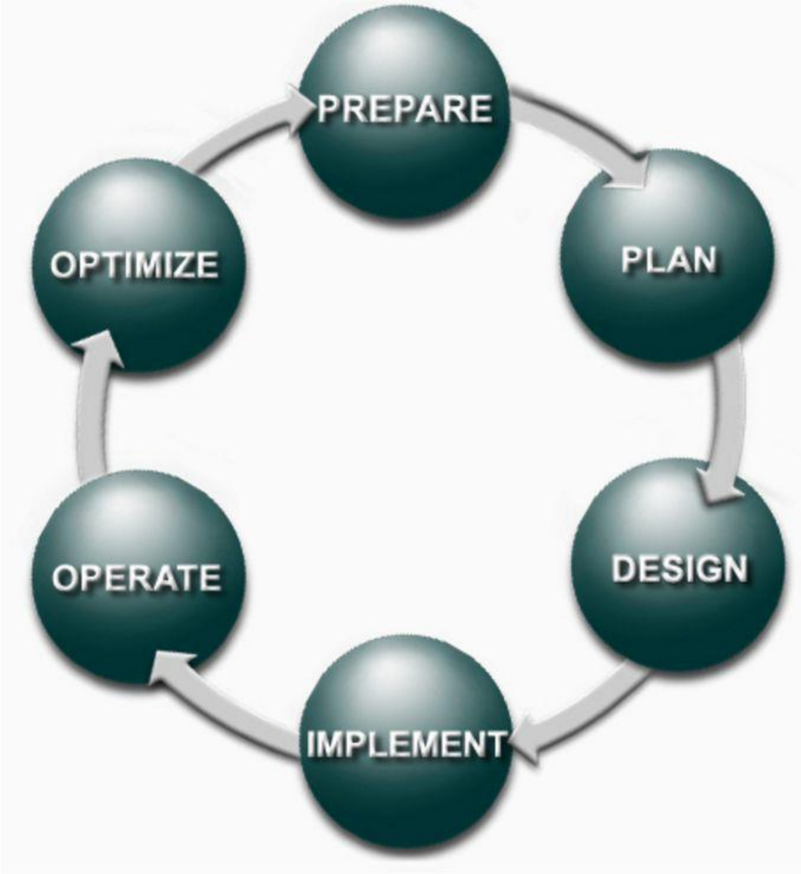
- **Systems Development Life Cycle (SDLC)**
- **Agile Software/Project Management**
- **PPDIOO (Cisco)**

PPDIOO – Network Life Cycle

- **Lower total cost of network ownership**
- **Increases network availability**
- **Improves business agility**
  - Stay competitive by add/move/change
    - ***Automation and DevOps***
- **Speeds access to applications and services**

PPDIOO – Network Life Cycle

- **Prepare**
- **Plan**
- **Design**
- **Implement**
- **Operate**
- **Optimize**



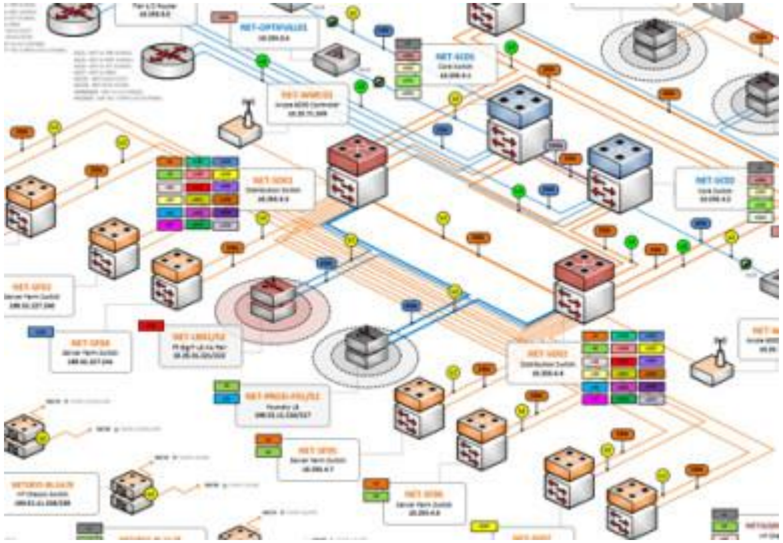
Fundamental Principles

- **Requirements gathering and characterizing the network**
  - Performance
  - Resilience
  - Scalability
  - Running Costs

- **Design Objectives, Guidelines, Principles**

Characterize the Network

- **Gather existing documentation and query**
- **Network audit**
- **Traffic analysis**
  - Netflow
  - NBAR
  - Captures
  - OpenFlow statistics
  - INT



Performance

- **Application response time**
  - What type of applications?
  - What is required for the applications to work?
  - How much bandwidth do they use--at any given time?

- **Delay tolerance**

- **Realtime communication**

- **Bandwidth**

- ***What does the company do?**
  - This creates a baseline for how the network needs to be designed

Sectors

- **Different design plans/options for companies**
  - Health Care
  - Restaurant/retail Chain
  - Non-profit
  - Security Company
  - Bank / Financial Institution
  - Government Agency
  - Startup

Resilience

- **Failover: Automatic vs manual**
  - What's the difference?
  - What's pro/con?
  - Convergence time (lower is better)
  - Automation & self-healing
  - Fail fast vs Fail proof

- **How much downtime is acceptable?**
  - This will vary for each company AND who you talk to at the company.
    - ***You should get multiple opinions?***

Scalability

- **Adequately supporting growth without having to re-design**

- **“Planning ahead”**
  - Number of users, networks, nodes, sites, etc.

- **Increased bandwidth**
  - What if there was twice the number of users, nodes, new applications, that demanded twice the bandwidth?

Scalability

- **The fundamental topology should not need to be redesigned to accommodate growth**

- **Increasing processing power/memory is acceptable; not a complete overhaul**
  - What networking paradigm makes this easier?

Running Costs (RC)

- **What is the current/future budget?**
- **Must meet technical requirements**
- **Must be cost effective**
  - Design and implementation
- **1) Cost vs. 2) performance vs. 3) availability**
  - Higher bandwidth
  - Backup/redundancy
  - Can only obtain 2/3

Running Costs

- **Good design is cost-effective to operate, and maintains consistent running costs**
  - What are some ways we can reduce CapEx/OpEx?
- **WAN typically highest RC**
- **Support is typically second highest RC**
  - Difficult to quantify
  - In house vs. third party?
  - Can we automate support?

Design Objectives

- **Set clear design objectives**
  - Performance targets

- **“Application” requirements**
  - Must understand ALL the requirements for ALL the applications at ALL times
    - ***Bandwidth consumption***
    - ***Sensitivity requirements***
    - ***Availability and downtime***
      - Nature of the business
        - » Financial
        - » Human life

Achieving Design Objectives

- **Requires practical and theoretical understanding of technologies**

- **Network support/implementation is needed before working in design roles?**
  - Scalable routing protocols
  - WAN transport
  - Network management and operations

- **Proof of concept (lab work)**
  - Too many variables to just be “on paper”
    - ***What can you do with the knowledge you have currently?***
    - ***Is this always the best option?***
  - Design, configure, demonstrate, implement (DCDI) cycle

Network Design Guidelines

- **Determine the performance parameters that best specify each of the design goals.**
  - For example, application response time, percentage packet loss, latency, and application availability.

- **Identify any design constraints.**
  - The most obvious constraint is budget.
  - Other constraints may include implementation timescale, support of legacy equipment, incorporation of specialized departments that require unique network specification and policy.

- **After considering the constraints, set targets for the relevant network performance parameters.**

- **Commence a high-level design (pseudo code)**
  - This is intended to resolve major issues such as the choice of WAN technology and equipment, the IP addressing plan, the degree to which routing is used instead of switching and so on.

Network Design Guidelines (continued)

- **Double-check this high-level design should then be compared to the constraints.**
  - If the constraints are not met an iterative step backwards is required. In the event of the constraints being met the design process can proceed.

- **A specific network design plan can now begin to be formulated.**
  - This addresses all technical details and alternatives for the design.

- **Each major aspect of the technical solution should be lab tested.**
  - The application response and availability characteristics should be tested in a lab. This will facilitate an iterative refinement of the technical solution.
    - ***Topology isolation > end-to-end test***

- **The design is complete when the technical design is fully refined.**
  - In some cases, the final lab tests may indicate that the fundamental performance targets or constraints are unrealistic and may have to be revised and compromised. It is however an aspiration to tentatively finalize these parameters at the high-level design stage.

Network Design Principles

- **Application drives design requirements**
  - Network facilitates the applications
    - ***This is why NetEng is so important!!***
  - Must understand the applications first before designing network

- **Experienced personnel**
  - Practical and theoretical hands-on experience with technologies and how they interact

- **Design is done on paper first, but must be tested in a lab**
  - Must be verified in a lab
    - ***Topology isolation > end-to-end test***
  - What if you don't test?
    - ***Pro/con***

Network Design Principles (cont.)

- **Trade-offs**
  - Cost, performance, availability

- **Vendor independence**
  - “Proprietary” solutions are often discouraged (Why?)
    - ***Vendor lock-in***
    - ***Open source***

- **Keep it simple**
  - Unnecessary complexity increase support cost (third party and in house)
    - ***Routing protocol example***

Network Design Principles (cont.)

- **Each network design is different**
  - No “cookie cutter” network designs between companies
    - ***When would this be good?***
  - Avoid cutting edge technologies

- **Predictability and consistency**
  - Performance, resilience, and scalability

- **Design it once—correctly**
  - Take the time to design it right
    - ***This includes automation***
  - Takes exponentially more time to redesign
  - Network diagram
    - ***“I can’t afford the time to make one.”***
    - ***“You can’t afford not to make one!”***

IP Addressing Plan & Routing

IP Addressing Plan

- **Foundation for successful and logical network design**

- **Support the network as it grows**
  - 2x to 10x (networks of the future!)

- **Choose correct routing protocol**
  - If routing protocol is needed!

Variable-length Subnet Masking (VLSM)

- **Implementing more than one mask on the same major class of network**
  - More efficient use of the address space for hosts and subnets
  - Essential on network with limited address space
    - ***Example***
  - Routing protocol must support it (classless)
    - ***Carry mask along with route advertisements***

Classless Routing Protocols

- **OSPF**
- **RIPv2**
- **EIGRP**
- **BGP**
- **IS-IS**

Example: IP Address Planning

- **172.16.0.0 /16**
  - 200 sites
    - ***400 point-to-point links***
    - ***100 hosts per site***

- **600 subnets; maximum of 100 hosts on any subnet?**

Example: IP Address Planning

172.16.0.0 /16
200 sites
400 point-to-point links
100 hosts per site

- **Find the shortest mask first (most hosts)**
  - Typically LAN segments
  - In our example: 7 bits (/25)
    - ***Easier/cleaner to use /24***
    - ***Rarely, if ever use anything greater that /24***

- **LANs – 172.16.1.0/24 to 172.16.200.0/24**

- **Subnet the subnets**
  - 172.16.201.0
    - ***/30 = 64 P2P***
    - ***172.16.201.x – 172.16.207.x/30***

- **Still have 172.16.208.0 – 172.16.255.x**

- **What's wrong with this network design? (in this example)**
  - Contiguous networks – why are they important?
  - Plan Ahead!

IPv6 Addressing

- **Stateful vs Stateless**
  - SLAAC vs DHCPv6
- **Subnetting**
- **Prefix-delegation**
- **Obtaining addresses from ISP**
  - Hardware restrictions
  - Dual-stack; tunneling

Route Summarization

- **Summarizing a group of routes into a single route advertisement**

- **Reducing size of routing tables**
  - Reduces latency (increased speed for route table look up; less entries)

- **Reduces routing protocol overhead (fewer routes advertised)**
  - Critical for growing networks

Summarization

- **Improves stability**
  - – No updates for single route changes
    - ***172.16.0.0/16***
      - – Not 172.16.33.0/24
  - – Speeds up convergence

- **Requires classless routing protocol**
  - – Plan non-conflicting summarization at strategic points
    - ***Example: router connects branch offices to HQ***
    - ***Subnets in range of 172.16.16.0/24 to 172.16.31.0/24***
    - ***Summarize 172.16.16.0/20***

Choosing the Routing Protocol

- **Stability**
  - Routing loops
  - Hold-down timers

- **Convergence speed**
  - Topology change
    - ***Inconsistent information***
    - ***LSA/LSD***

- **Metric**
  - Multiple paths to a destination
    - ***Load-balancing***
  - Different protocols use different metrics to decide best path to destination
    - ***Hop count, administrative cost, AS path, etc.***

Choosing the Routing Protocol

- **VLSM**
  - – Classless routing protocols

- **Route summarization**
  - – Must support summarization
    - ***Auto-summarization can be bad!***
      - – RIPv1
      - – Assumes no subnetting; summarized routes may be in conflict

Choosing the Routing Protocol

- **Classful versus Classless**

- **Scalability**
  - Routing protocol adequately support network operation as the network grows
  - Convergence speed, VLSM, route summarization, etc.
  - Why is RIPv1 not scalable?

IPAM, NSOT, & Change Management

- **IPAM**
  - – Software?

- **Network Source of Truth**

- **IaC**

- **How do you do change management?**
  - – Authorization and Authentication

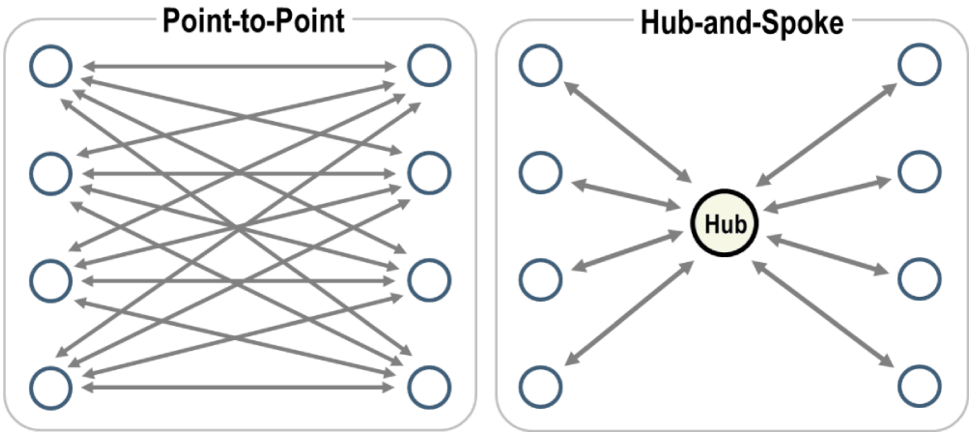
LAN Design

Switching Network Design

- **Collision domains**
- **Forwarding**
- **Traffic filtering and forwarding**
  - Security
    - ***802.1x***
    - ***AAA***

Design Layout Options

- **Hub and spoke**
- **Daisy chain**
- **Star/full mesh**
- **Clos**



Design Objectives

- **Understand client-server traffic flow**
  - Traffic profiles
    - ***What clients are talking to what servers***
    - ***How long, and how much bandwidth now and in the future?***
    - ***How do we determine this?***
      - Netbrain
      - Thousandeyes
      - SD-WAN

- **High-speed core**
  - 802.3ad (Link Aggregation)
  - Hardware
    - ***Cost?!***

Virtual LANs (VLANs)

- **Broadcast containment**
  - IP addressing plan
- **Security**
  - Inter-VLAN communication
- **Flexibility**
  - Combine intelligence of a routed network with flexibility of a switched LAN
  - Multiple switches (trunks)
  - Layer 3 switch
- **What are some limitations/issues with VLANs?**

VLANs

- **VLAN planning**
  - Across campus network
  - Maintain consistency
  - Configuration in physical switch (or use protocol--GVRP)
- **VLAN range**
  - Single wiring closet
  - Each floor is VLAN
  - Server farm
    - ***Latency***
  - How many hosts per VLAN?
    - ***Scalability***
- **Number of VLANs**
- **Number of users per VLAN**

Optimizing Spanning Tree (STP)

- **port fast; edgeport; etc.**
  - – RSTP
  - – SPB
- **Root bridge**
  - – Carefully, manually select (why?)
- **PVST**
  - – One root vs. multiple
    - ***Why/why not?***

Clos Leaf/Spine

IP Telephony (VoIP)

- **Voice traffic on separate VLAN**
  - Performance and security
  - Distinguishable (troubleshooting and management)

- **Power to phones**
  - PoE vs external power

- **Cabling**
  - One drop

Designing the WAN

Choosing the WAN Technology and Internet Connection

- **Single biggest expense**
- **Cost versus performance tradeoff**
- **Internet connection versus WAN connection**

WAN Design

- **Cost**
- **Speed**
  - Bandwidth vs. Latency
- **Location**
  - Services available

WAN Design

- **Application and business functionalities**

- **Organization Priorities**
  - Failover
  - Redundancy
  - Disaster Recovery
  - Data Center

Internet and WAN

- **Each site has local Internet connection**
  - Reduces link at HQ
  - Also be used for failover
  - No policing

- **Some sites have local Internet**

- **No sites have local Internet**
  - Large Internet link at HQ
  - Large hardware devices
  - Central site policing/monitoring

WAN Design Options

- **Access technologies**
  - Legacy - Frame Relay, ATM, DSL
  - MPLS, Metro Optical Ethernet (MOE) / fiber, “business class” cable (IPsec)
  - SD-WAN
- **Point to Point**
  - T1, T3, serial, layer 2 (Metro-Ethernet)
  - Private (eVPN)
  - Dedicated
- **Hub and spoke**
- **Full mesh**
- **Phone service**
  - VoIP, Analog, or both

Critical Topics

- **Data Center**
  - Hosted vs onsite
  - Cloud
    - ***Private vs public vs mixed***
    - ***Disaster recovery/failover***
  - Storage & compute

- **SDN**
  - Traditional to SDN transition
  - Greenfield (add as you go)

- **DevOps & automation**
  - IaC
  - CI/CD
  - Test environment
    - ***Considerations***

Security

- **Planning**
- **Mitigation strategies**
- **Incident response**
- **Remediation strategies**
- **Backups and backup plan**
- **Securing the network and devices**

- **Policies**
- **Technical**
  - Best practices
    - ***VPN, AAA, 802.1X, etc.***
- **Physical**
  - Key card
  - Access control

Questions?