Top-Down Network Design

Chapter Twelve

Testing Your Network Design

1

Reasons to Test

- Verifying that the design meets key business and technical goals.
- Validating LAN and WAN technology and device selections.
- Verifying that a service provider provides the agreed-upon service.
- Identifying any bottlenecks or connectivity problems.
- Testing the redundancy of the network.
- Analyzing the effects on performance of network link failures.
- Determining optimization techniques that will be necessary to meet performance and other technical goals.

2

Reasons to Test

- Analyzing the effects on performance of upgrading network links or devices ("what-if analyses").
- Proving that your design is better than a competing design.
- Passing an "acceptance test" that gives you approval to go forward with the network implementation
- Convincing managers and coworkers that your design is effective.
- Identifying any risks that might impede implementation and planning for contingencies.
- Determining how much additional testing might be required

3

Testing Your Network Design

- Use industry testing services
- Build and test a prototype system
- Use third-party and Cisco tools

4

Industry Testing Services

- The Interoperability Lab at the University of New Hampshire (IOL)
- ICSA Labs
- Miercom Labs
- KeyLabs
- The Tolly Group
- Most tests are component tests, rather than system tests. Component testing is generally not sufficient to measure the performance of a network design.
- Furthermore, the test configuration used by the vendor or testing lab almost certainly does not match your actual configuration.

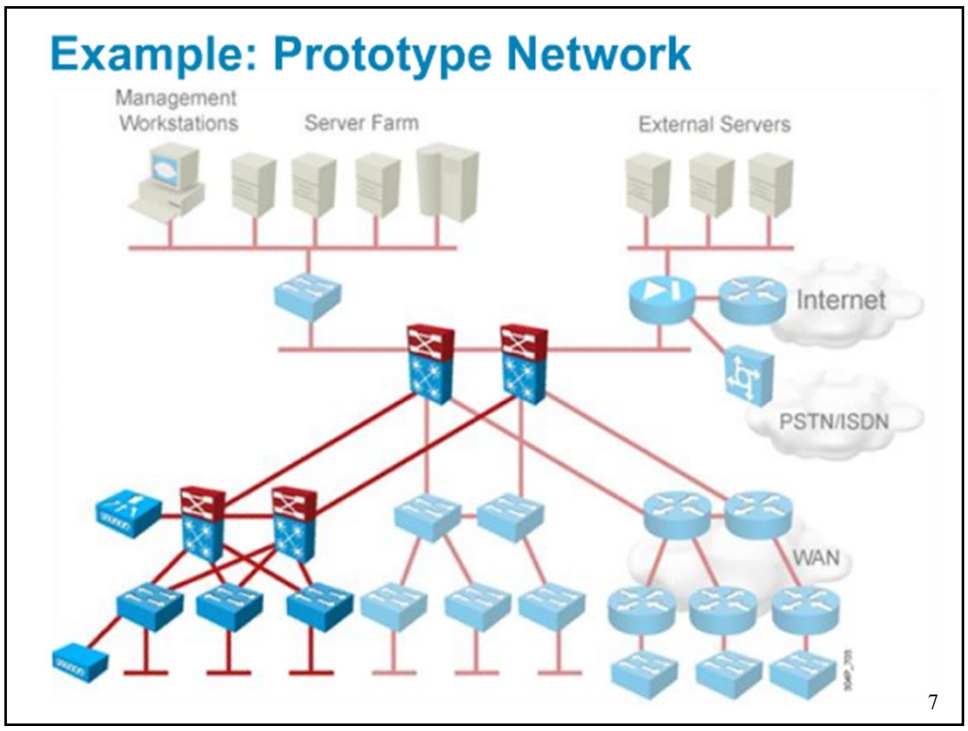
5

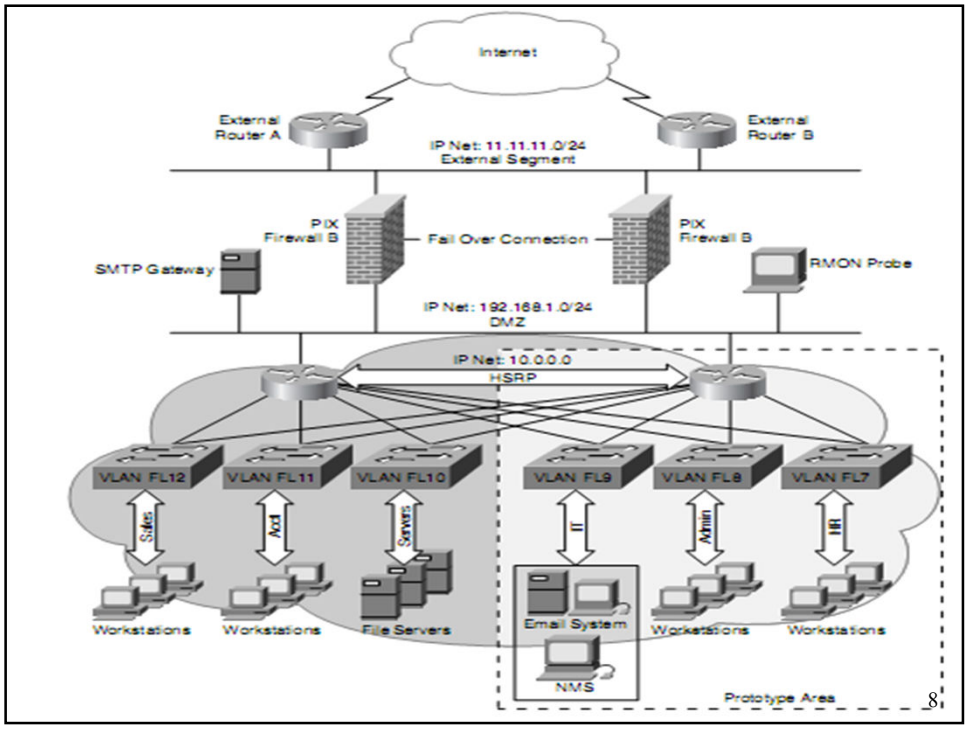
Prototype System - Scope

A prototype is an initial implementation of a new system that provides a model on which the final implementation will be patterned.

- It's not generally practical to implement a full-scale system
- A prototype should verify important capabilities and functions that might not perform adequately
- Risky functions include complex, intricate functions and functions that were influenced by the need to make tradeoffs

6


Example: Prototype Network
Management Workstations
Server Farm
External Servers
Internet
PSTN/ISDN
WAN
7


Internet
External Router A
External Router B
IP Net: 11.11.11.0/24
External Segment
PIX Firewall B
Fail Over Connection
PIX Firewall B
SMTP Gateway
RMON Probe
IP Net: 192.168.1.0/24
DMZ
IP Net: 10.0.0.0
HSRP
VLAN FL12
VLAN FL11
VLAN FL10
VLAN FL9
VLAN FL8
VLAN FL7
Sales
Acct
Servers
IT
Admin
HR
Workstations
Workstations
File Servers
Email System
NMS
Workstations
Workstations
Prototype Area
8

Components of a Test Plan

- Test objectives and acceptance criteria
- The types of tests that will be run
- Network equipment and other resources required
- Testing scripts
- The timeline and milestones for the testing project

9

Test Objectives and Acceptance Criteria

- Specific and concrete
- Based on business and technical goals
- Clear criteria for declaring that a test passed or failed
- Avoid biases and preconceived notions about outcomes
- If appropriate, reference a baseline

10

Types of Tests

- Application response-time tests - measures performance from a user's point of view and evaluates how much time a user must wait when executing typical operations that cause network activity.
- Throughput tests - measures throughput for a particular application in KBps or MBps.
- Availability tests - tests are run for 24 to 72 hours, under medium to heavy load. The rate of errors and failures are monitored.
- Regression tests - makes sure the new system doesn't break any applications or components that were known to work and perform to a certain level before the new system was installed.

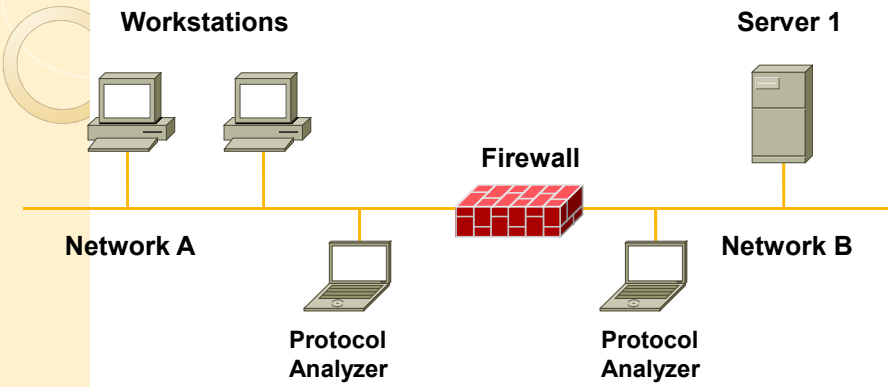
11

Resources Needed for Testing

- Scheduled time in a lab either at your site or the customer's site
- Power, air conditioning, rack space, and other physical resources
- Help from coworkers or customer staff
- Help from users to test applications
- Network addresses and names

12

Example Test Script



- Test objective. Assess the firewall's capability to block Application ABC traffic, during both light and moderately heavy load conditions.
- Acceptance criterion. The firewall should block the TCP SYN request from every workstation on Network A that attempts to set up an Application ABC session with Server1 on Network B. The firewall should send each workstation a TCP RST (reset) packet.

13

Example Test Script (continued)

1. Start capturing network traffic on the protocol analyzer on Network A.
2. Start capturing network traffic on the protocol analyzer on Network B.
3. Run Application ABC on a workstation located on Network A and access Server1 on Network B.
4. Stop capturing network traffic on the protocol analyzers.
5. Display data on Network A's protocol analyzer and verify that the analyzer captured a TCP SYN packet from the workstation. Verify that the network layer destination address is Server1 on Network B, and the destination port is port 1234 (the port number for Application ABC). Verify that the firewall responded to the workstation with a TCP RST packet.

14

Example Test Script (continued)

6. Display data on Network B's protocol analyzer and verify that the analyzer did not capture any Application-ABC traffic from the workstation.
7. Log the results of the test in the project log file.
8. Save the protocol-analyzer trace files to the project trace-file directory.
9. Gradually increase the workload on the firewall, by increasing the number of workstations on Network A one at a time, until 50 workstations are running Application ABC and attempting to reach Server1. Repeat steps 1 through 8 after each workstation is added to the test.

15

Tools for Testing a Network Design

- Network-management and monitoring tools
- Traffic generation tools
- Modeling and simulation tools
- QoS and service-level management tools
- http://www.topdownbook.com/tools.html
- Simulation is the process of using software and mathematical models to analyze the behavior of a network without requiring an actual network.
- A simulation tool lets you develop a model of a network, estimate the performance of the network, and compare alternatives for implementing the network.

16

Writing Test Scripts

- Write a script of how the test will be run. Include
  - Test objectives
  - Acceptance criterion
  - Test steps

17

Documenting the Project Timeline

- For complex testing projects the test plan should document the project timeline, including start and finish dates for the project and major milestones

18

Implementing the Test Plan

- Follow the test scripts
- Document your work
- Keep a daily activity log

19

Summary

- An untested network design probably won't work
- It's often not practical to test the entire design
- However, by using industry testing services and tools, as well as your own testing scripts, you can (and should) test the complex, risky, and key components of a network design

20

Top-Down Network Design

Chapter Thirteen

Optimizing Your Network Design

21

Reasons to Optimize

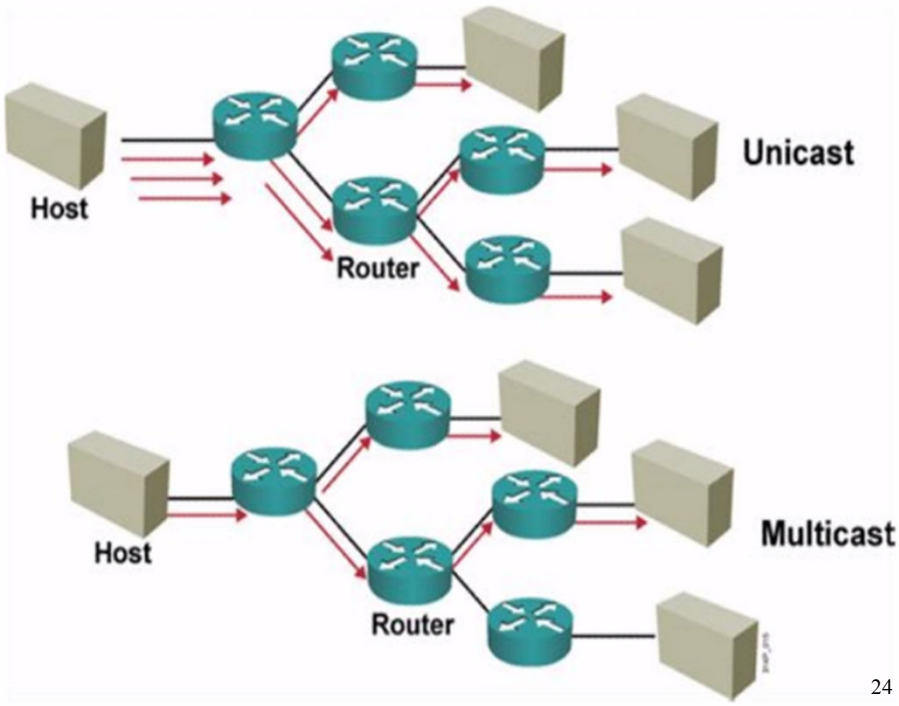
- Meet key business and technical goals
- Use bandwidth efficiently
- Control delay and jitter
- Reduce serialization delay
- Support preferential service for essential applications
- Meet Quality of Service (QoS) requirements

22

Optimizing Bandwidth Usage with IP Multicast Technologies

- High-bandwidth multiple-user multimedia
  - distance learning, videoconferencing and collaborative computing
- Old way - send a data stream to every user
- Alternative - use a single stream and use a broadcast destination address
  - Disadvantages - goes to all devices
- Multicast - single data stream only stations that request

23



24

IP Multicast Addressing

- Transmits IP data to a group of hosts that are identified by a single Class-D IP address (224.0.0.0 to 239.255.255.255)
- Can also be identified by a MAC-layer multicast address. Optimizes network performance since it allows NICs to ignore data streams

25

The Internet Group Management Protocol (IGMP)

- Allows a host to join a group and inform routers of the need to receive a particular data stream
- Host transmits a membership-report message
- Multicast router sends an IGMP query out every port periodically
- To lessen bandwidth host sets a random timer to reply to IGMP query
- IGMPv2 - recognizes when last host has left a group

26

A Few Technologies for Meeting QoS Requirements

- IETF controlled load service
- IETF guaranteed service
- IP precedence
- IP differentiated services

27

Optimizing Network Performance to Meet Quality of Service Requirements

- Two types
  - Controlled-load service
    - provides a client data flow with a QoS closely approximating the QoS that the flow would receive on an unloaded network
  - Guaranteed service
    - provides firm bounds on end-to-end packet queuing delays. Guaranteed for applications that need it

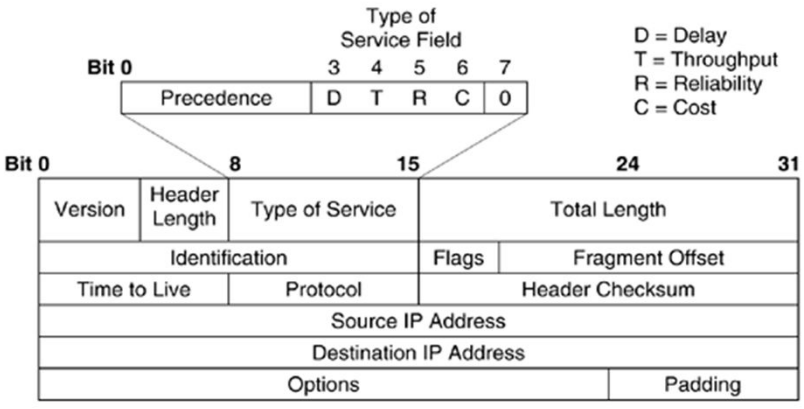
28

IP Precedence and Type of service

- Specifies both precedence and type of service
  - Precedence - helps router determine which packets to send when several packets are queued
  - Type of service helps router select a routing path when multiple paths are available
- Type-of-service byte: 3 bit precedence and 4 bit type-of-service

29

IP Type of Service Field

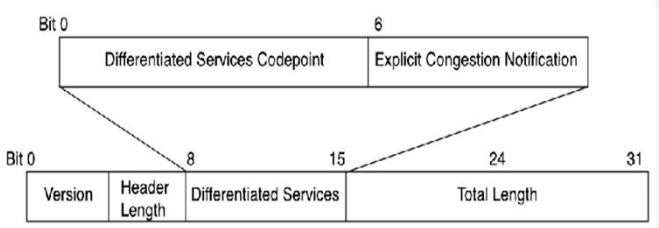


The delay bit (D). Tells routers to minimize delay
The throughput bit (T). Tells routers to maximize throughput
The reliability bit (R). Tells routers to maximize reliability
The cost bit (C). Tells routers to minimize monetary cost

30

IP Differentiated Services (DS) Field

- RFC 2474 redefines the type of service field as the Differentiated Services (DS) field
  - Bits 0 through 5 are the Differentiated Services Codepoint (DSCP) subfield
    - Has essentially the same goal as the precedence subfield
    - Influences queuing and packet dropping decisions for IP packets at a router output interface
  - Bits 6 and 7 are the Explicit Congestion Notification (ECN) subfield



31

Real-Time Protocol

- Used by multimedia applications
- Provides end-to-end network transport functions suitable for transmitting real-time data
- Usually runs on top of User Datagram Protocol (UDP)
- Relies on lower layer services to deliver QoS

32

Reducing Serialization Delay

The time to output a packet is called transmission delay or serialization delay on a slow WAN link.

- Link-layer fragmentation and interleaving
  - Breaks up and reassembles frames
- Compressed Real Time Protocol
  - Compressed RTP compresses the RTP, UDP, and IP header from 40 bytes to 2 to 4 bytes

33

Classifying LAN Traffic

- IEEE 802.1p specifies mechanisms for switches to expedite the delivery of time-critical traffic and to limit the extent of high-bandwidth multicast traffic within a switched LAN.
- Classifies traffic at the data-link layer
- Supports eight classes of service
- A switch can have a separate queue for each class and service the highest-priority queues first

34

Cisco Switching Techniques

- Process switching
- Fast switching
- Autonomous, silicon, and optimum switching
- NetFlow switching
- Cisco Express Forwarding (CEF)

35

Classic Methods for Layer-3 Packet Switching

- Process switching is the slowest of the switching methods. Processor interrupted to process packet information
- Silicon switching speeds up autonomous switching by using silicon switching cache
- Optimum switching is faster due to an enhanced caching algorithm and the optimized structured of the cache
- Distributed switching supports very fast throughput because the switching process occurs on the interface card

36

NetFlow Switching

- New switching that is optimized for environments where services must be applied to packets to implement security, QoS features, and traffic accounting
- Identifies traffic flows and then quickly switches packets in the flows when it applies services

37

Cisco Express Forwarding

- Technique for switching packets very quickly across large backbones networks and the Internet
- Evolved to accommodate Web-based applications and other interactive applications that are characterized by session of short duration to multiple destinations addresses

38

Cisco Queuing Services

Allows a network device to handle an overflow of traffic using queuing methods

- First in, first out (FIFO) queuing
- Priority queuing
- Custom queuing
- Weighted fair queuing (WFQ)
- Class-based WFQ (CBWFQ)
- Low latency queuing (LLQ)

39

First In, First Out Queuing

- Basic store and forward functionality
- Stores when network is congested and forwards them in order
- Provides no QoS functionality

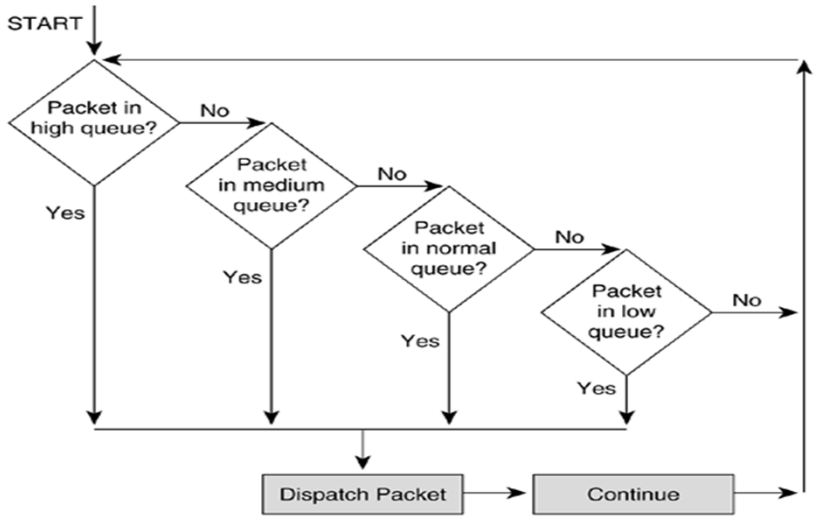
40

Priority Queuing

- Ensures that important traffic is processed first
- Designed to give strict priority to a critical application
- Is appropriate where WAN links are congested from time to time
- Has four queues: high, medium, normal and low

41

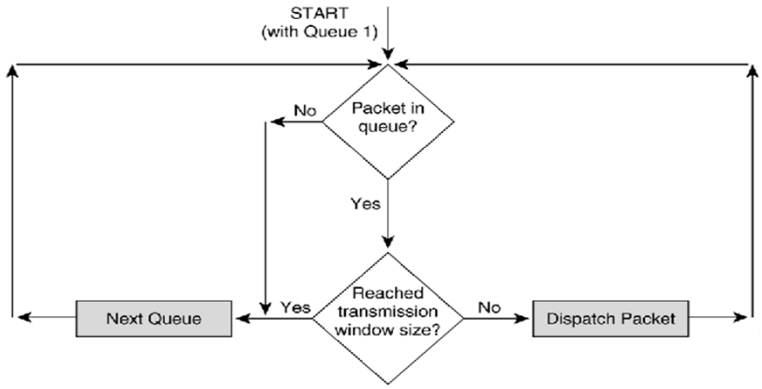
Priority Queuing



42

Custom Queuing

- Designed to allow a network to be shared among applications with different minimum bandwidth or latency requirements
- Assigns different amounts of queue space to different protocols and handles the queues in round-robin order



43

Weighted Fair Queuing

- Sophisticated set of algorithms designed to reduce delay variability and provide predictable throughput and response time for traffic flows
- Goal is to offer uniform service to light and heavy network users alike
- Recognizes an interactive application and schedules that traffic to the front of the queue
- Adapts automatically to changing network traffic conditions and requires little or no configuration
- Can allocate bandwidth based on precedence

44

Random Early Detection (RED)

- Congestion avoidance rather than congestion management
- Monitors traffic loads and randomly discards packets if congestion increases
- Source nodes detect dropped packets and slow down
  - Works best with TCP

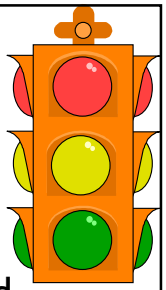
45

Weighted Random Early Detection

- Combines the capabilities of standard RED algorithm with IP precedence
- Provides preferential traffic handling for higher-priority packets
- Selectively discards lower priority traffic

46

Low-Latency Queuing



- One queue always gets the green light
  - Use this for voice
- Combine this with class-based weighted fair queuing
  - Define traffic classes based on protocols, access control lists, and input interfaces
  - Assign characteristics to classes such as bandwidth required and the maximum number of packets that can be queued for the class

47

Traffic Shaping

- Allows management and control of network traffic to avoid bottlenecks and meet QoS requirements
- Avoids congestion by reducing outbound traffic for a flow to a configured bit rate while queuing bursts to that rate
- Configured on a per-interface basis
- Avoid overwhelming a downstream router or link

48

Committed Access Rate (CAR)

- Cisco feature for classifying traffic on an incoming interface
- Can drop a packet or change the IP precedence or DSCP bits
- Supports specifying policies regarding how traffic that exceeds a certain bandwidth allocation should be handled
- Looks at received traffic, compares it to a configured maximum and takes action based on the result

49

Summary

- Optimization provides the high bandwidth, low delay, and controlled jitter required by many critical business applications
- To minimize bandwidth utilization by multimedia applications, use IP multicast
- To reduce serialization delay, use link fragmentation and compressed RTP
- To support QoS and optimize performance, use IP precedence, DSCP, 802.1p, advanced switching and queuing methods, RED, CAR, etc.

50

Top-Down Network Design

Chapter Fourteen

Documenting Your Network Design

51

Documenting Your Design

- If you are given a request for proposal (RFP), respond to the request in the exact format that the RFP specifies
- If no RFP, you should still write a design document
  - Describe your customer's requirements and how your design meets those requirements
  - Document the budget for the project
  - Explain plans for implementing the design

52

Typical RFP Response Topics

- A network topology for the new design
- Information on the protocols, technologies, and products that form the design
- An implementation plan
- A training plan
- Support and service information
- Prices and payment options
- Qualifications of the responding vendor or supplier
- Recommendations from other customers
- Legal contractual terms and conditions

53

Contents of a Network Design Document

- Executive summary
- Project goal
- Project scope
- Design requirements
- Current state of the network
- New logical and physical design
- Results of network design testing
- Implementation plan
- Project budget

54

Executive Summary

- States the major points of the document. It should be no more than one page and should be targeted at the managers and key project participants who will decide whether to accept your design.
- The goal is to sell the decision-makers on the business benefits of your design.
- Technical information should be summarized and organized in order of the customer's highest-priority objectives for the design project.

55

Project Goal

State the primary goal for the network design project. The goal should be business oriented and related to an overall objective. The Project Goal section should be no more than one paragraph.

An example:

The goal of this project is to develop a wide-area network (WAN) that will support new high-bandwidth and low-delay multimedia applications. The new applications are key to the successful implementation of new training programs for the sales force. The new WAN should facilitate the goal of increasing sales in the United States by 50 percent in the next fiscal year.

56

Project Scope

Provides a summary of the departments and networks that will be affected by the project.

New network or modifications. For a single network segment, a set of LANs, a building or campus network, a set of WAN or remote-access networks, or possibly the whole enterprise network.

An example:

The scope of this project is to update the existing WAN that connects all major sales offices in the United States to corporate headquarters. The new WAN will be accessed by sales, marketing, and training employees. It is beyond the scope of this project to update any LANs that these employees use. It is also beyond the scope of this project to update the networks in satellite and telecommuter offices.

57

Design Requirements

- Business goals explain the role the network design will play in helping an organization succeed
- Technical goals include scalability, performance, security, manageability, usability, adaptability, and affordability

58

Logical and Physical Design

- Logical design
  - Topology
  - Models for addressing and naming
  - Switching and routing protocols
  - Security strategies
  - Network management strategies
- Physical design
  - Actual technologies and devices

59

Implementation Plan

- Recommendations for deploying the network design
- Project schedule
  - Including any dates and times for service provider installations
- Any plans for outsourcing
- Training
- Risks
- A fallback plan if the implementation should fail
- A plan for evolving the design as new requirements arise

60

Possible Appendixes

- Detailed topology maps
- Device configurations
- Addressing and naming details
- Network design testing results
- Contact information
- Pricing and payment options
- More information about the company that is presenting the design
  - Annual reports, product catalogs, press releases
- Legal contractual terms and conditions

61

Detailed Structure of a Design Document

Design Document Index
1. Introduction
2. Design requirements
3. Existing network infrastructure
   - 3.1. Network topology
   - 3.2. Network audit
   - 3.3. Applications used in the network
   - 3.4. Network health analysis
   - 3.5. Recommended changes to the existing network
4. Design
   - 4.1. Design summary
   - 4.2. Design details
     - 4.2.1. Topology design
     - 4.2.2. Addressing design
     - 4.2.3. EIGRP design
     - 4.2.4. Security design
     - . . .
   - 4.3. Implementation details
     - 4.3.1. Configuration templates for campus devices
     - 4.3.2. Configuration templates for WAN devices
     - . . .
5. Proof of concept
   - 5.1. Pilot or prototype network
   - 5.2. Test results
6. Implementation plan
   - 6.1. Summary
   - 6.2. Implementation steps

Appendix A—List of existing network devices
Appendix B —Configurations of existing network devices

62

Summary

- When a customer provides an RFP, make sure to follow the prescribed format
- When not bound by an RFP, develop a design document that describes requirements, the existing network, the logical and physical design, an implementation plan, and the budget
- Be sure to include an executive summary
- In some cases, include appendixes with detailed information

63

Review Questions

- Why is it important to test your network design?
- Why is regression testing important?
- What are some characteristics of well-written acceptance criteria?
- What are some characteristics of a good network simulation tool?

64

Review Questions

- Why is it important to optimize your network?
- What has become of the IP type of service field?
- What are some methods for marking packets to identify the need for priority handling?
- Compare and contrast Cisco queuing services.

65

Review Questions

- Why is it important to document your network design?
- Why is it important to submit an RFP proposal in the exact format prescribed?
- What are the major topics in a design document?
- What are some possible appendixes for a design document?

66

