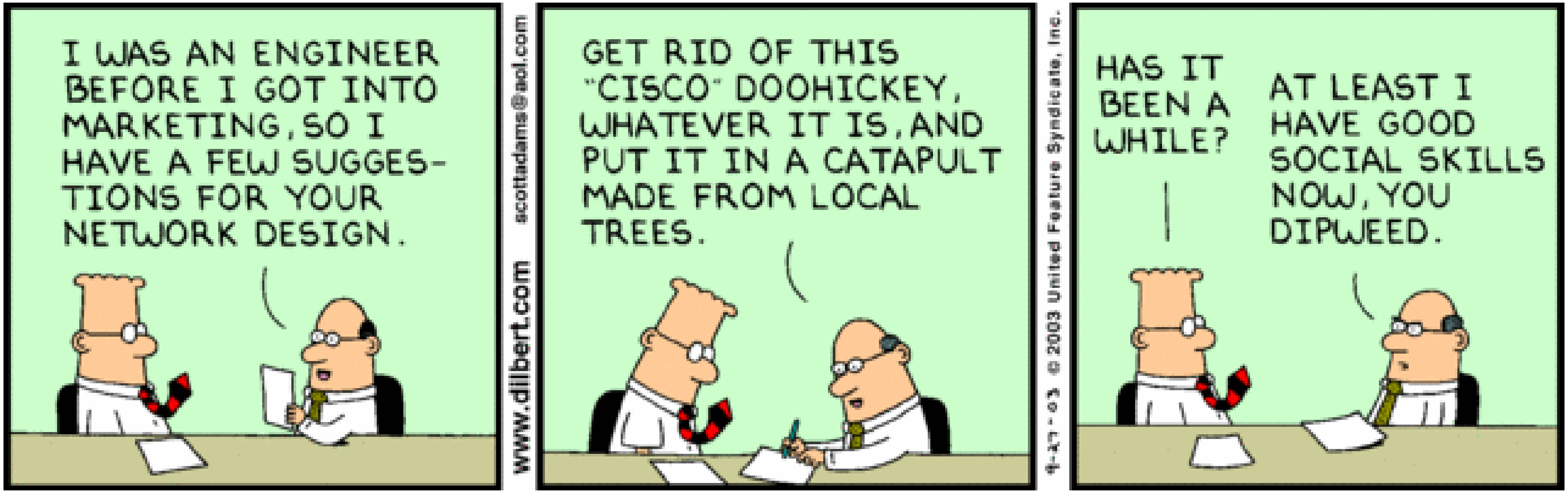
A Top-Down Approach for Network Designs Aligned to Business Goals

Network Design Methodology

Freddy Bello M, CCIE 1840
fbello@netxar.com
www.netxar.com


I WAS AN ENGINEER BEFORE I GOT INTO MARKETING, SO I HAVE A FEW SUGGESTIONS FOR YOUR NETWORK DESIGN.
www.dilbert.com
scottadams@aol.com
GET RID OF THIS "CISCO" DOOHICKEY, WHATEVER IT IS, AND PUT IT IN A CATAPULT MADE FROM LOCAL TREES.
9-27-03 © 2003 United Feature Syndicate, Inc.
HAS IT BEEN A WHILE?
AT LEAST I HAVE GOOD SOCIAL SKILLS NOW, YOU DIPWEED.

Source www.dilbert.com ®

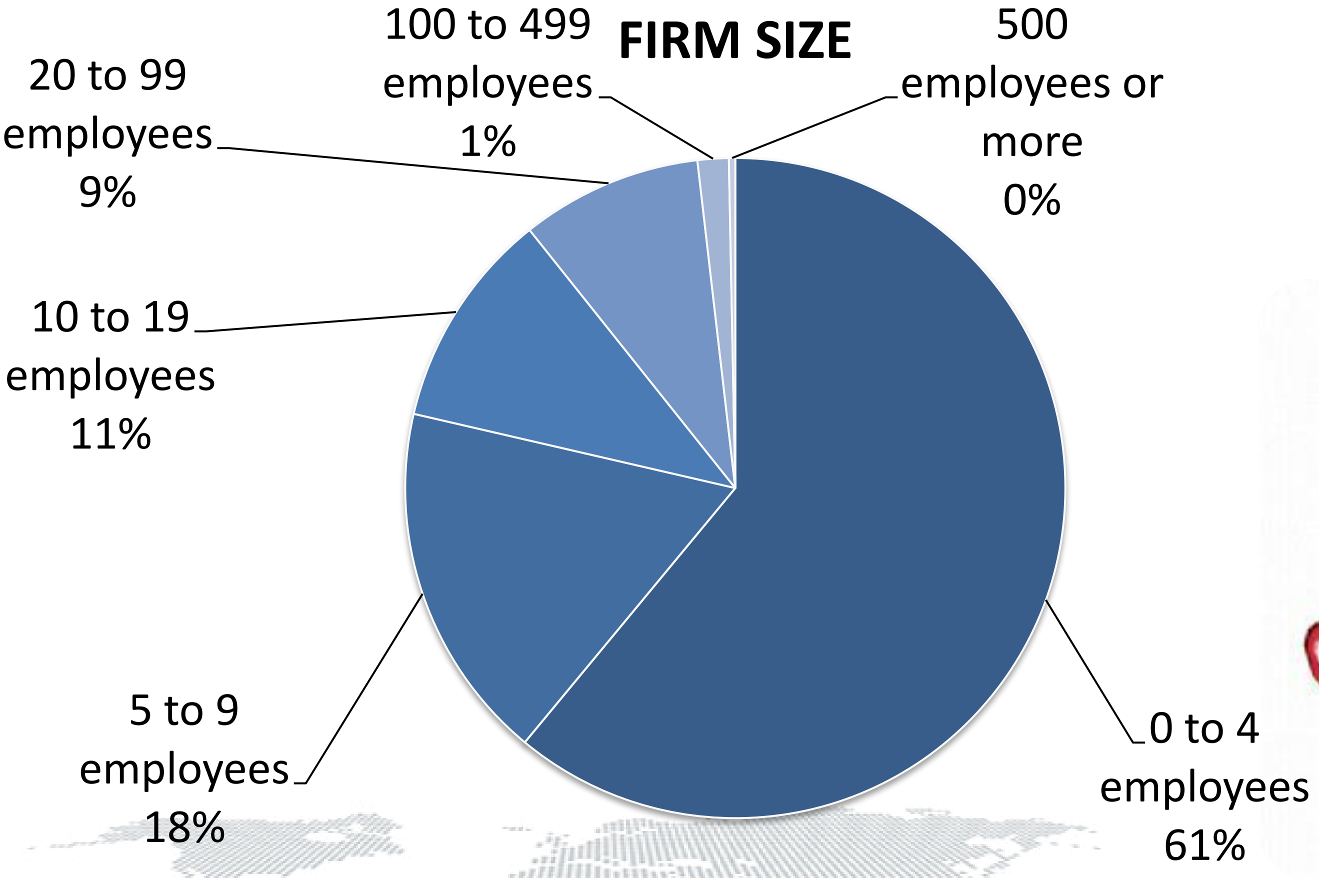
Objectives of This Section

- **Learn**
  - How to design a network using the correct techniques
  - Some common guidelines used to evaluate a network design

Organization Size

- Books and articles in the trade make you think that every organization is huge
- That each one has a highly complex network with multiple layer of equipment

Organization Size



Network Size

- The network needed by most organizations is therefore fairly small
- A single broadcast domain can work just fine with several hundred active users

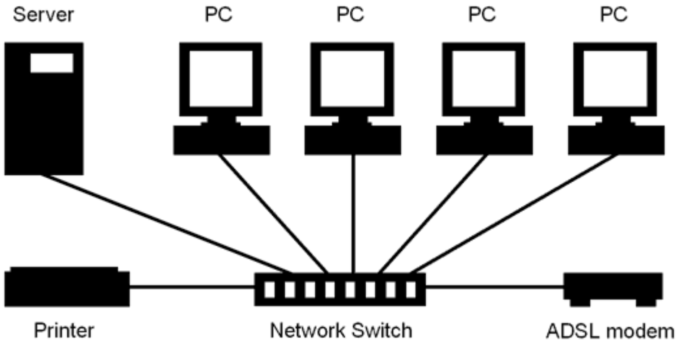
REALITY CHECK

Network Size

- In term is network size here are some guidelines
  - Small
    - 200 or fewer end devices
  - Medium
    - 200 to 1,000 end devices
  - Large
    - More than 1,000 end devices

SOHO

- 1 to 19 employees
- Represent 98 percent of all firms
- No need more than a single local area network consisting of a single switch, a server or NAS box, and a printer



SMB

- Small and Medium sized businesses are defined as those with 500 or fewer employees
- Organization with up to 500 staff in a single location could also work well with a single or at worst a handful of local area networks, a set of switches, a server, maybe separate storage, and a number of printers

Large

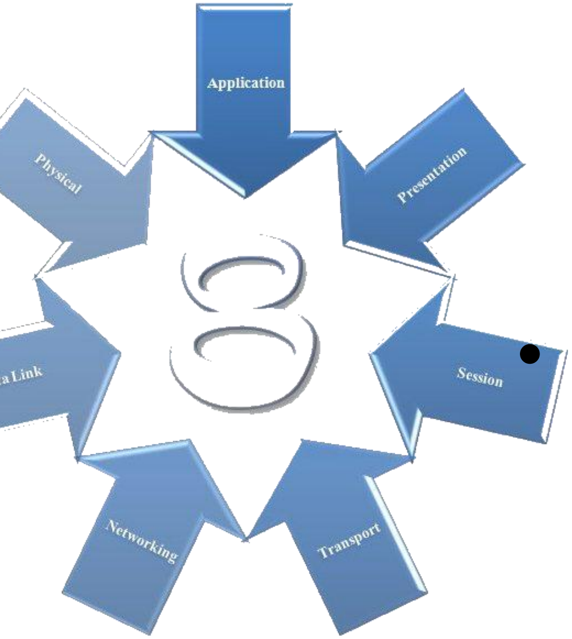
- This leaves just 1% organizations with 500 or more employees out of over total of firms

Do Not Over Complicate

- **What is the point to this discussion?**
  - To point out to you to not over complicate this
  - A **basic, simple, single layer network** design will work for over 98 percent of all firms

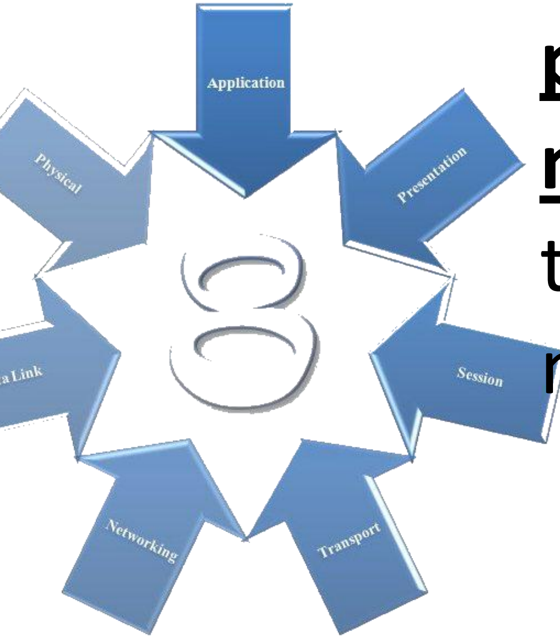
KEEP IT SIMPLE, STUPID (AND SHORT) - KISS

Approach to Network Design



- The approach in this presentation will be on the necessity to account for all seven layers of the OSI model when creating a design for a network
- As well as accounting for that all important eighth layer, in other words **the political factors that always have an effect on any technical decision**

Approach to Network Design

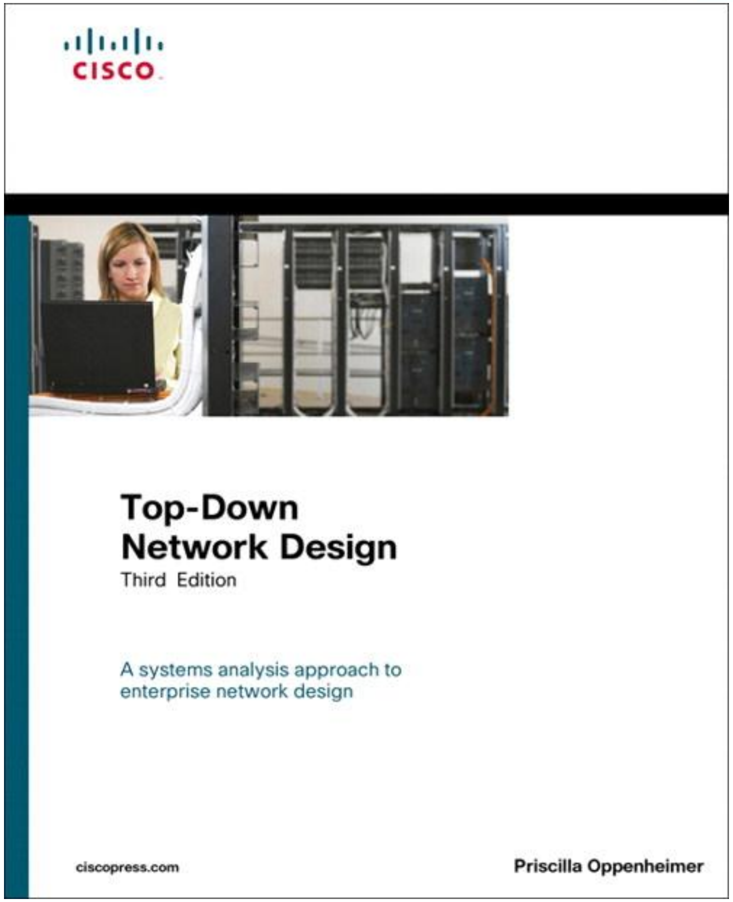


- Network design **<u>must be a complete process that matches business needs to the available technology</u>** to deliver a system that will maximize the organization

What is the Point to This

- The first consideration is what will the network be sharing and with whom
- Whatever needs to be shared and with whom, will determine the type and scope of the network

The Framework



Top-Down Network Design

Third Edition

A systems analysis approach to enterprise network design

ciscopress.com

Priscilla Oppenheimer

- The framework that will be used here is based on **Top Down Network Design Third Edition** by Priscilla Oppenheimer from Cisco Press

Oppenheimer Steps

- **Identifying Customer Needs/Goals**
  - Analyzing Business Goals and Constraints
  - Analyzing Technical Goals and Tradeoffs
  - Characterizing the Existing Network
  - Characterizing Network Traffic

Oppenheimer Steps

- **Logical Network Design**
  - – Designing a Network Topology
  - – Designing Models for Addressing and Naming
  - – Selecting Switching and Routing Protocols
  - – Developing Network Security Strategies
  - – Developing Network Management Strategies

Oppenheimer Steps

- **Physical Network Design**
  - – Selecting Technologies and Devices for Campus Networks
  - – Selecting Technologies and Devices for Enterprise Networks

Oppenheimer Steps

- **Testing Optimizing Documenting**
  - – Testing the Network Design
  - – Optimizing the Network Design
  - – Documenting the Network Design

Identifying Customer Needs/Goals

Business Goals and Constraints

- The first thing to do is to understand the business goals for the project, such as
  - Why are we here
  - What advantage to the business will this project bring

Business Goals and Constraints

- It is also important to understand the business constraints,ie
  - What we want is an unlimited budget and time to work
  - But we will not get this

Collect Information

- The next step is to ensure that before meeting with the client, whether internal or external some basic business related information has been collected
  - Competition
  - Market Conditions
  - Future of the Industry
  - Products Produced/Services Supplied
  - Financial Condition

Meet With the Customer

- Once the basic information has been collected, meet with the customer to hear what they have to say
- At that meeting, collect information on the project

Meet With the Customer

- Specifically try to get
  - A concise statement of the goals of the project
    - Problem to be solved
    - New capability to be added
    - What has the competition just done to them
  - What must happen for the project to be a success

Meet With the Customer

- What will happen if the project is a failure
  - Is this a critical business function
  - Is this just something they want to try
  - Do they really think it will work
- Get a copy of the organization chart
  - This will show the general layout of the organization
  - It will suggest users to be accounted for
  - It will suggest geographical locations to account for

Meet With the Customer

– Find out about biases the customer has

– For example

- Will they only use certain companies products
- Do they avoid certain things
- This applies to the technical and management staff

Gather Information at the Site

- Once all of the basic information has been collected, it is time to start gathering information at the site concerning the actual project
- This information begins with information on the applications
  - List all the applications that cross the network
    - Now and after the project is completed
    - Both productivity and management applications

Application List

Application Name	Application Type	New Existing	Importance	Notes
MAS90	Enterprise accounting	Existing	Critical	A new version that switches from client/server to browser/server will be out in one month
Quicken	Accounting	Existing	Low	CEO uses for home budget
OpenView	System	Existing	High	Monitors routers
MRTG	System	New	High	Produces network usage data

Business Constraints

- Constraints on the project might include those related to business practices, such as
  - The security of the facility
  - When can work be done

Business Constraints

- Other constraints might relate to their staff
  - What of their staff can you use
  - When can you use their staff
  - What is the level of competence of their staff, as they may be more of a problem than a help
- The timeframe is always a constraint
  - Due dates
  - Milestones

Technical Goals and Tradeoffs

- Besides the business goals and constraints, it is important to understand the technical goals
- The technical tradeoffs must be understood as well
- Oppenheimer lists eight things to consider

Scalability

- Scalability refers to what is needed today as well as the future
- The ability to grow, for example
  - Cabling is meant to last for 10 years
  - Switches and routers are meant to last for 2 to 5 years, since it is easier to change these
- Get an idea of the needs for next 2 to 5 years

Scalability

- At least you need to know
  - Number of sites to be added
  - What will be needed at each of these sites
  - How many users will be added
  - Where might servers be located
  - New lines of business
- This is not the current project, but perhaps only things dimly in the future

Availability

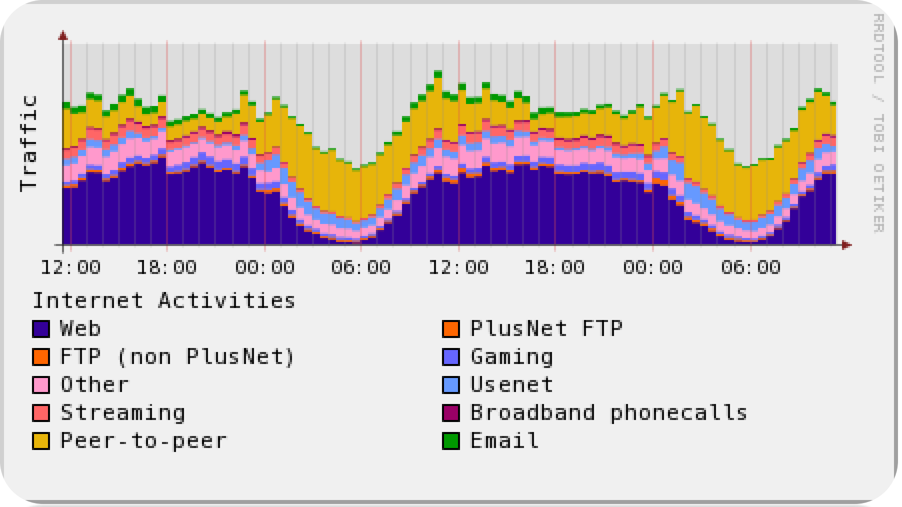
- Availability is the uptime
- It is expressed as a percent and is related to the time period
    - Such as
        - 99% per minute
        - 95% per month
- Small variations translate into big times
- Different applications may require different levels

Performance

- Performance is a key indicator for most projects
- In some cases it is only that
  - “No one complains”
- In most cases it is more definitive

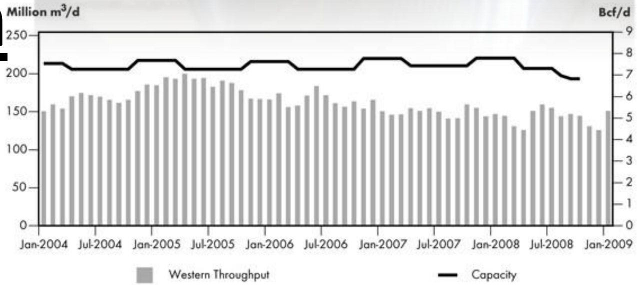
Performance

- Common performance measures include
  - Capacity v Throughput
  - Bandwidth Utilization
  - Offered Load
  - Accuracy
  - Efficiency
  - Latency
  - Response
  - Device CPU Utilization



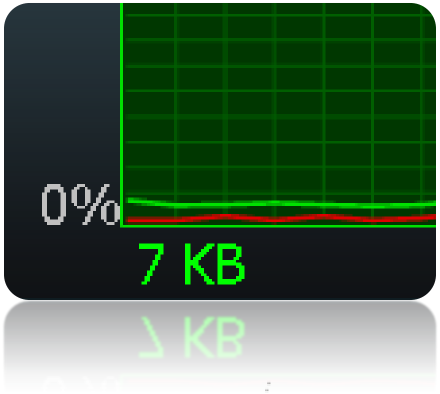
Capacity v Throughput

- Capacity is **<u>what the link is capable of</u>**
  - – Commonly stated as the pipe size, such as 1.544 Mbps
- Throughput is the measured **<u>quantity of data going through the pipe</u>**
  - – Throughput is usually less than capacity, but it could be the same as the capacity, at least in theory

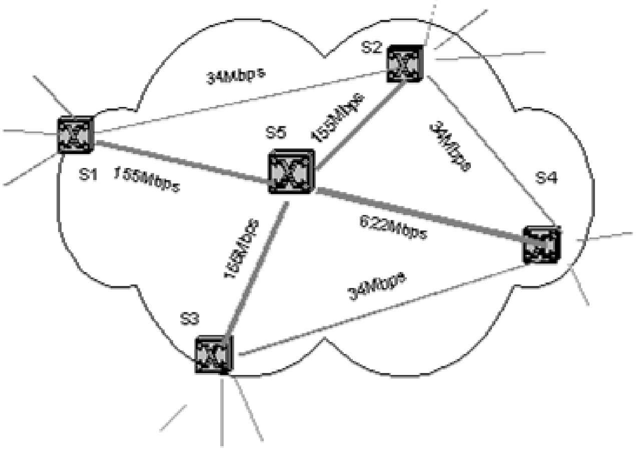


Performance

- **Bandwidth Utilization**
  - The percent of total available capacity in use



- **Offered Load**
  - This is the sum of all the data all network devices have ready to send at a particular time

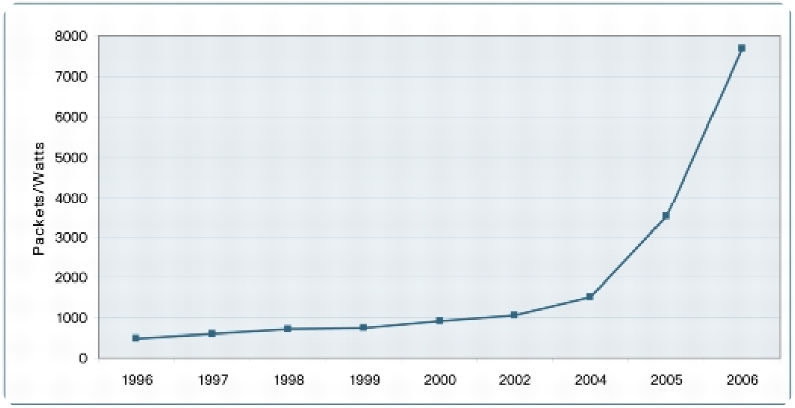


Performance

- **Accuracy**
  - Exactly what goes out gets to the other end
  - To check accuracy use a network analyzer to check the CRC on received frames
  - Track the number of frames received with a bad CRC every hour for one or two days
  - It is normal for errors to increase as network utilization goes up
  - The error rate is acceptable if there are not more than one error per megabyte of data

Performance

- **Efficiency**
  - How much overhead is required to deliver an amount of data
  - How large a packet can be used
    - Larger better
    - Too large means too much data is lost if a packet is damaged
    - How many packets can be sent in one bunch without an acknowledgment



Performance

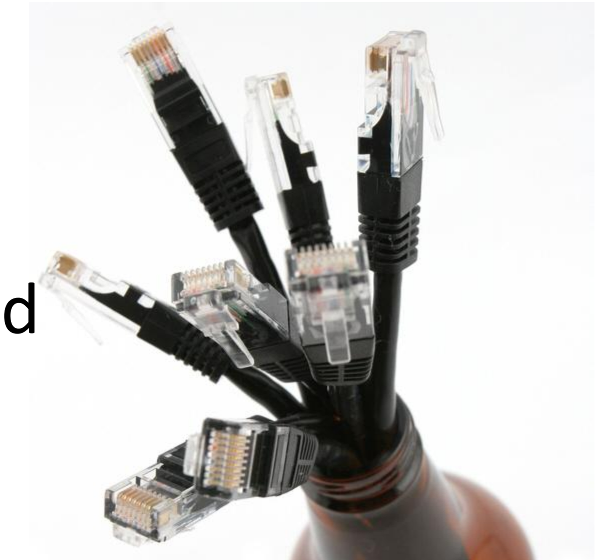
- **Latency**
  - This is the delay in transmission
  - The time that passes from when a user expects something to appear, to when it does appear
  - Instantaneous response is the only goal

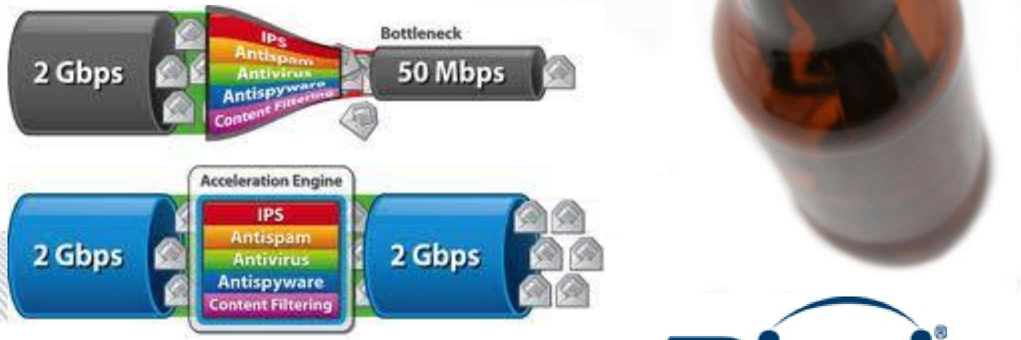
Performance

- **Response**
  - Related to latency, but also a function of the application and the equipment the application is running on
  - Most users expect to see something on the screen in 100 to 200 milliseconds

Performance

- **Device CPU Utilization**
  - High utilization on a device may create a bottleneck as the device will be unable to handle the offered load regardless of the bandwidth coming in or going out of the device



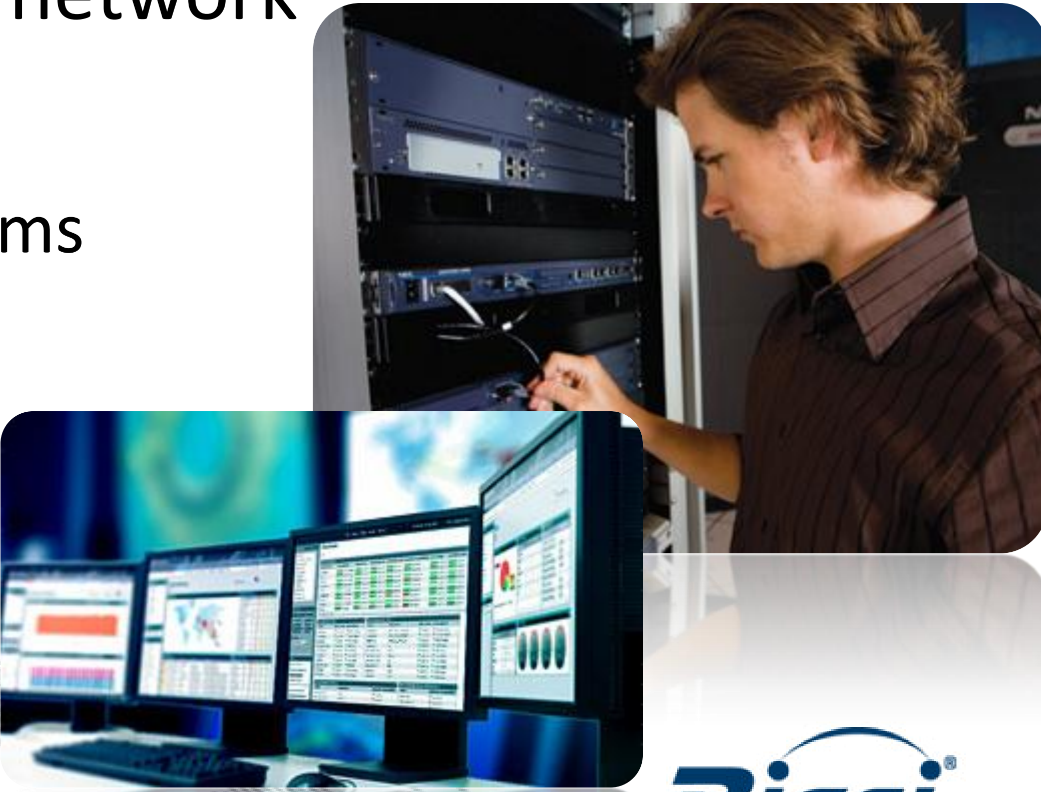


Security

- In assessing the amount of security, balance the risks against the cost
- There is no point in locking things down so tight, nothing can be used
- Common risks include
  - Use of resources
  - Loss of data
  - Alteration of data
  - Denial of service

Manageability

- Manageability refers to how easy will it be to monitor the network
- To check for
  - – Performance problems
  - – Errors
  - – Security problems
  - – Configuration
  - – Accounting



Ease of Use

- How difficult will it be for the network management team to run the network you will leaving
- How difficult will it be for the network team to change the network by themselves

Adaptability

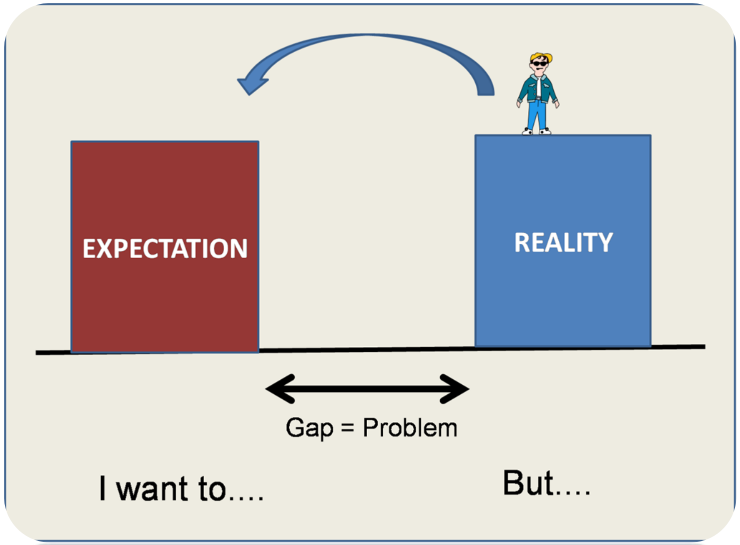
- A network must be adaptable
- Can the network change as circumstances change
- Proprietary technologies reduce adaptability
- Standards are preferred if possible

Affordability

- Do not propose a network they cannot pay for
- It must be affordable
- Find out the budget in the beginning
- Adhere to the budget
- Get all change orders approved in writing before changes are made

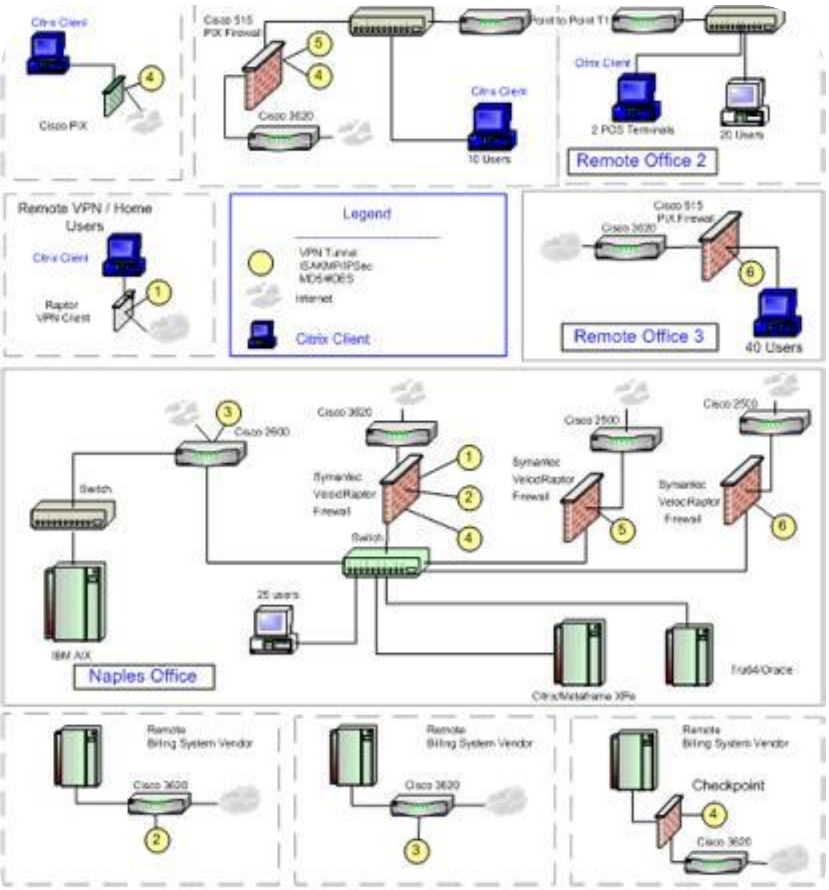
The Existing Network

- We now know where we want to go based on the analysis that was just done
- We next need to determine where we are starting from



Information to Collect

- A network map is the first thing to work on
- This map should include
  - Geographic locations
  - WAN connections between sites
    - Labeled with type/speed/protocols/media/ISP
  - Buildings and floors where equipment will be
  - Connections between buildings and floors
    - Labeled with type/speed/protocols/media

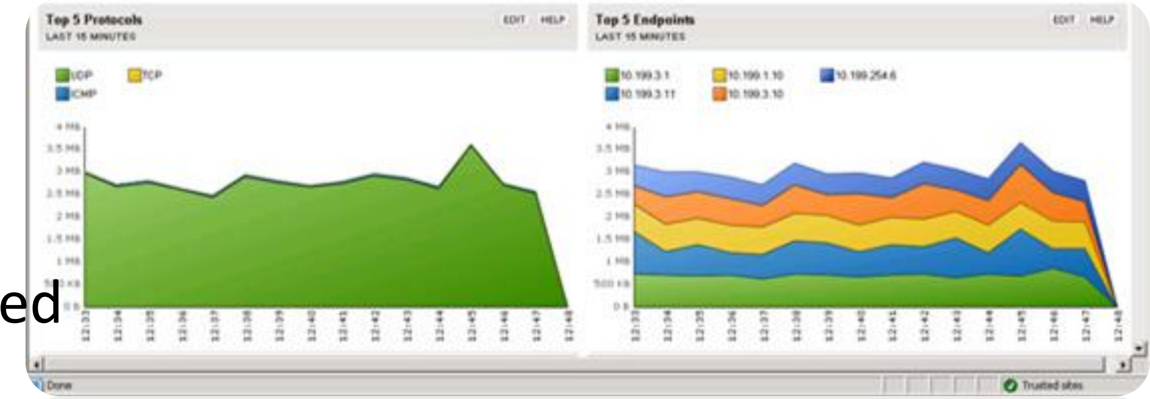


Information to Collect

  - Location of connection points like routers and switches
  - Internet connections
  - Remote access points
- **A baseline will be needed as this will tell you where the network is today**

Information to Collect

- **Measure**
  - Bandwidth utilization by time of day and protocol
    - Be sure to account for print jobs, especially large ones
  - Errors per MB of data
  - Response time
    - Pings may be used for this



Information to Collect

- **Trend Analysis**
  - Collect the same basic information discussed in baselining, but do this over time
  - It also allows you to justify buying new toys at the end of the year when a budget surplus is discovered and must be spent quickly

Characterizing Network Traffic

- In this step the flow of the traffic both existing and to be added or changed will be accounted for
- This is done by identifying
  - Sources and destinations of traffic
  - Direction and type of flow between these points
  - Volume of traffic

User Community List

Community Name	Number of Users	Location	Application
Enterprise Accounting	5	Building B Floor 2 Rooms 3-5	MAS90
CEO Accounting	1	Building A Corner Office	Quicken
Network Managers	3	Building C Deep Dark Basement	OpenView
Network Managers	3	Building C Deep Dark Basement	AlertPage

Data Stores List

Data Store Name	Location	Application	Used By
Accounting Data	Building C Even Deeper and Darker Basement	MAS90	Enterprise Accounting
CEO's Budget	Building A Corner Office	Quicken	CEO
OpenView Logs	Building C Deep Dark Basement	OpenView	Network Managers
AlertPage Logs	Building C Deep Dark Basement	AlertPage	Network Managers

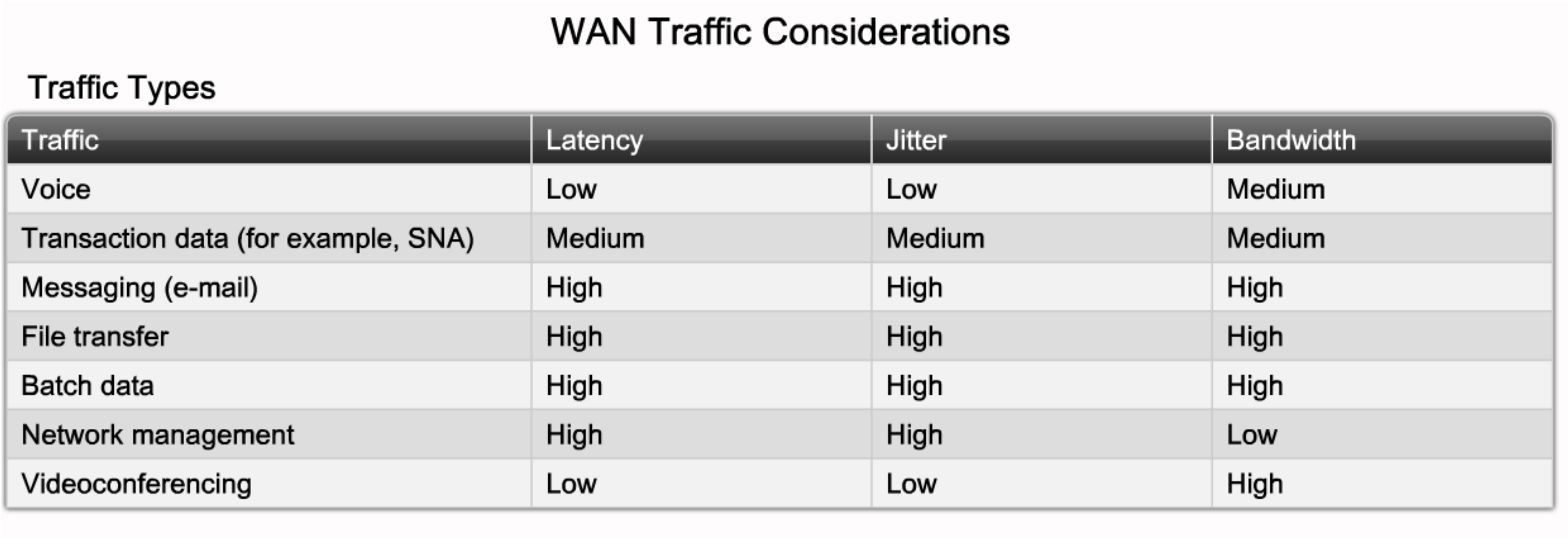
Collecting Network Traffic

- For the data flow from the user communities to their data stores, measure or estimate the traffic flow over the links
- Use a network analyzer or network management tool for this
- This is not likely to be exact
- It is being used to identify bottlenecks

Collecting Network Traffic

- The type of traffic is important
- This will influence the type of link required
- At this stage the QoS is important as well since it will affect the type of link
  - Only some link types can support QoS
- Again a chart is used to collect this information

Types of Traffic



WAN Traffic Considerations

Traffic Types

Traffic	Latency	Jitter	Bandwidth
Voice	Low	Low	Medium
Transaction data (for example, SNA)	Medium	Medium	Medium
Messaging (e-mail)	High	High	High
File transfer	High	High	High
Batch data	High	High	High
Network management	High	High	Low
Videoconferencing	Low	Low	High

Types of Traffic

- Different traffic types have different characteristics
  - Terminal/Host
    - Asymmetrical
    - Terminal sends a few characters
    - Host sends back many characters
  - Client/Server
    - Similar to above
    - Client sends more data as does the server

Types of Traffic

- Browser/Server
  - Similar to a terminal/server
  - Uses a web browser instead of a dedicated program
  - The server response will be quite large possibly
- Peer-to-Peer
  - This flow is bi-directional and symmetric
  - Unix-to-Unix workstations often use this

Types of Traffic

- Server-to-Server
  - The flow depends on the relationship between the servers
  - If mirrored, then one way and high level
  - Other relationships may be more bi-directional
- Distributed Computing
  - Several computers join together to solve a single problem
  - Normally the exchange is quite high
  - It is bi-directional and symmetrical

Type of Traffic List

Application	Type of Traffic	Protocol	User Community	Data Store	Bandwidth	QoS
Enterprise Accounting	Client/Server Browser/Server	IP	Enterprise Accounting	Accounting Data	Average of 2 Mbps from 8 to 5 weekdays	None
Note this is blank	Because the CEO's	Quicken Data	Does not leave CEO's office	NA	NA	NA
OpenView	Terminal/Server	IP	Average of 2 Kbps 24X7X365	OpenView Logs	Average of 2 Kbps 24X7X365	None
AlertPage	Terminal/Server	IP	Average of 65 Kbps Every hour 24X7X365	AlertPage Logs	Average of 65 Kbps Every hour 24X7X365	None

Types of Traffic

- A quick estimate of traffic flow can be made by using the following table
- This table shows the average flows for the different types of data
- In many cases, especially when tools such as a baselining tool or protocol analyzer are not available, this is the best that can be done

Traffic Flow Estimates List

Type of Application	Typical Data Size Kbytes	Type of Application	Typical Data Size Kbytes
Terminal Screen	4	Graphical Screen	500
Email	10	Presentation Document	2,000
Web Page	50	High Resolution Image	50,000
Spreadsheet	100	Multimedia Object	100,000
Word Processing Document	200	Database	1,000,000

Measuring Traffic Flow

- How do you actually determine what size data lines are required
- This is often difficult and inexact

Environmental Considerations

- In addition to network traffic there are other factors that must be taken into account
- For example is the site able to support the environmental load
- These factors include such things as
  - Electrical load
  - Air conditioning
  - Heating
  - Ability to place new cables

PoE

- PoE – Power Over Ethernet is a standard from the IEEE
  - This 802.3af standard specifies how electrical power can be delivered to end user devices through the data cable
- PoE can place an unusually heavy electrical load on the LAN room
- Most equipment rooms are not wired for this type of load

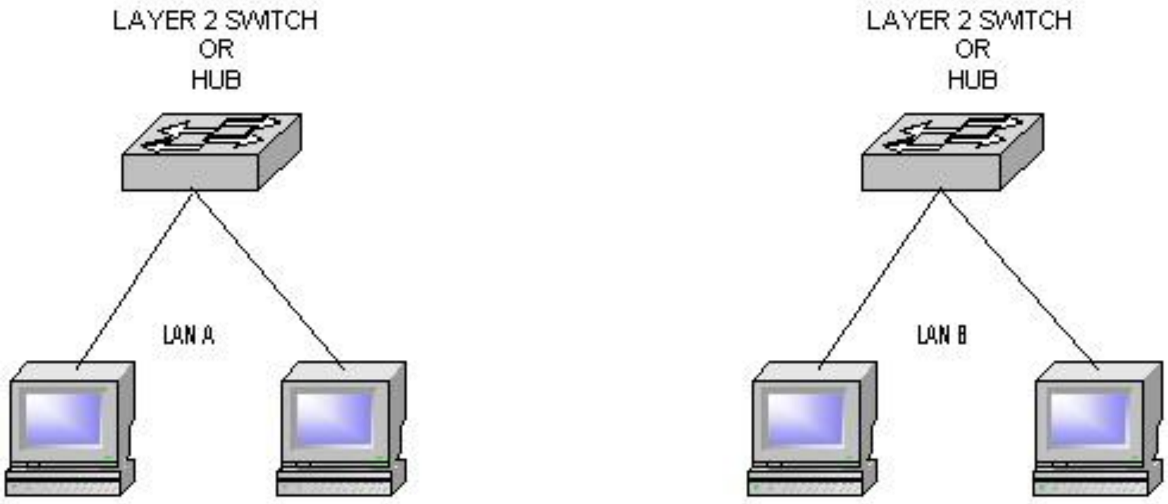
Logical Network Design

Designing a Network Topology

- Network design is an art, not a science
- There are no absolutes
- There are no precisely correct formulas
- **It always depends**
- There are two basic types of network designs
  - Flat
  - Hierarchical

Flat Network

- In a flat network all connecting devices are on the same level

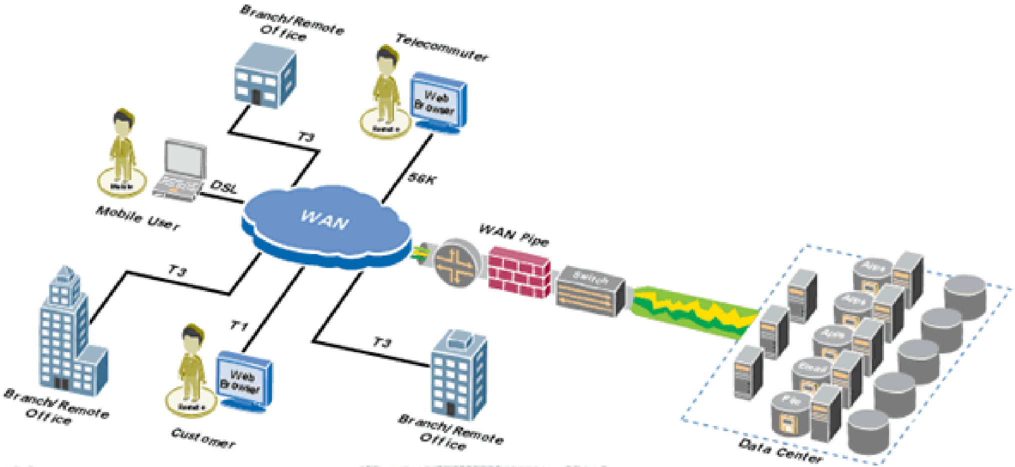


Flat Network Design

- A flat design is appropriate for a small and static network
- A flat network is a single collision domain or one that is not divided hierarchically
- There is a limit to the number of stations that can be supported in a flat design
- Broadcast domains are divided using
  - Layer 3 Switches
  - Routers

Hierarchical Network

- In a hierarchical design all connecting devices are still on the same level, but these are interconnected at a level above it



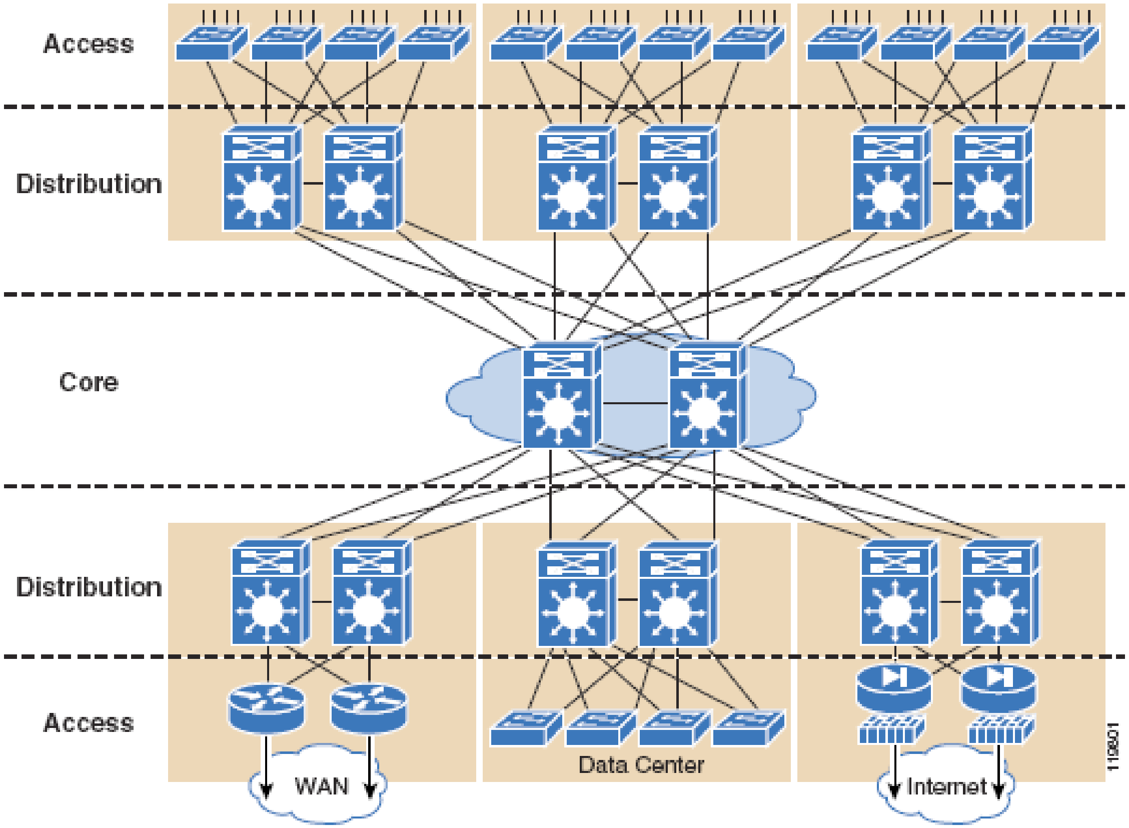
Hierarchical Types

- In the Cisco world any network design is hierarchical
- This is so the network can be
  - Organized
  - Managed
  - Scaled
  - Upgraded

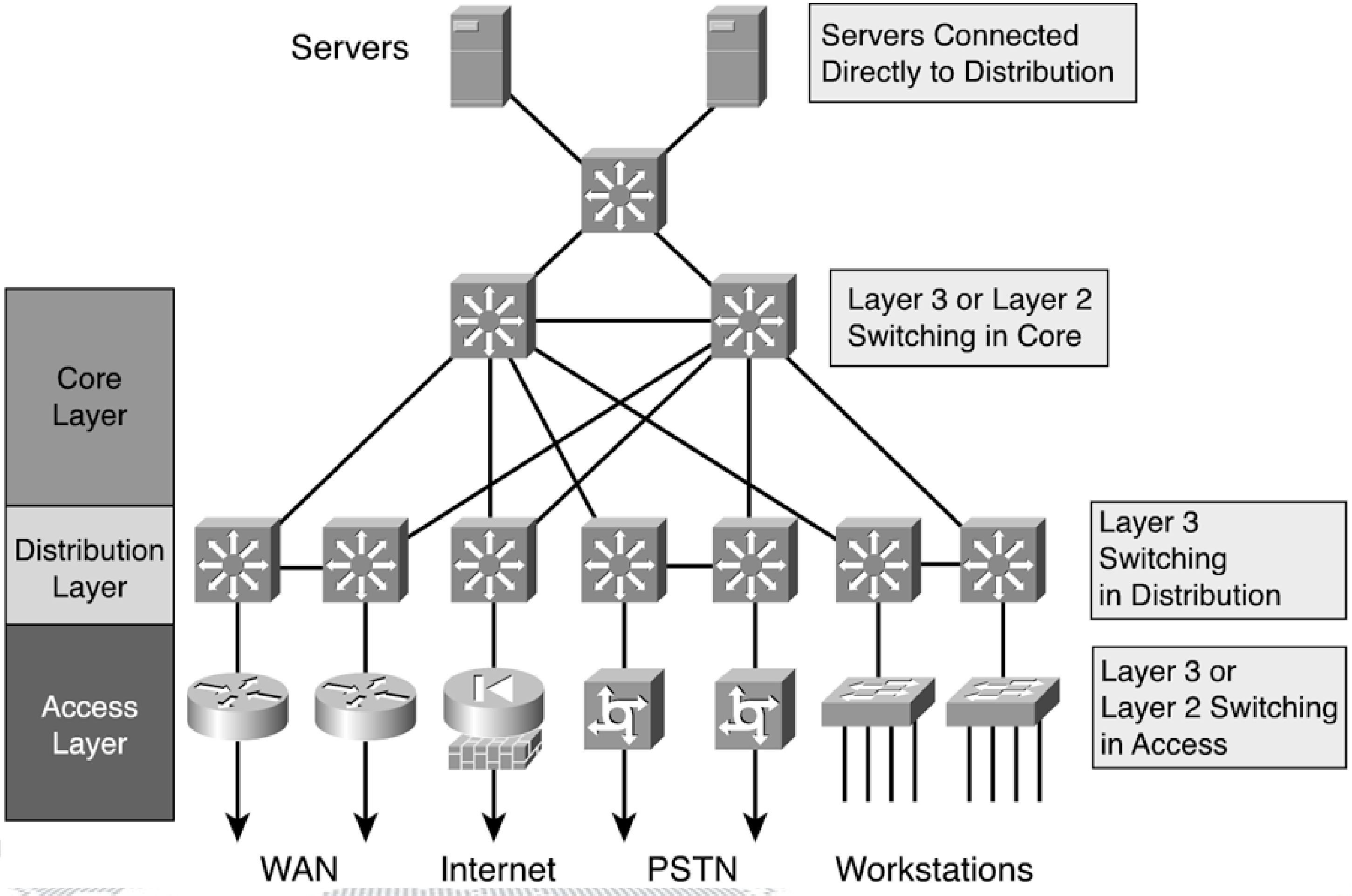
Network Design Hierarchy

- In the traditional Cisco network design model there are three basic levels
  - – Access
    - Where switching is the primary activity
  - – Distribution
    - Where routing occurs
  - – Core
    - Which forms a backbone for connecting the distribution level segments of larger networks

The Layers


Access
Distribution
Core
Distribution
Access
WAN
Data Center
Internet
119801

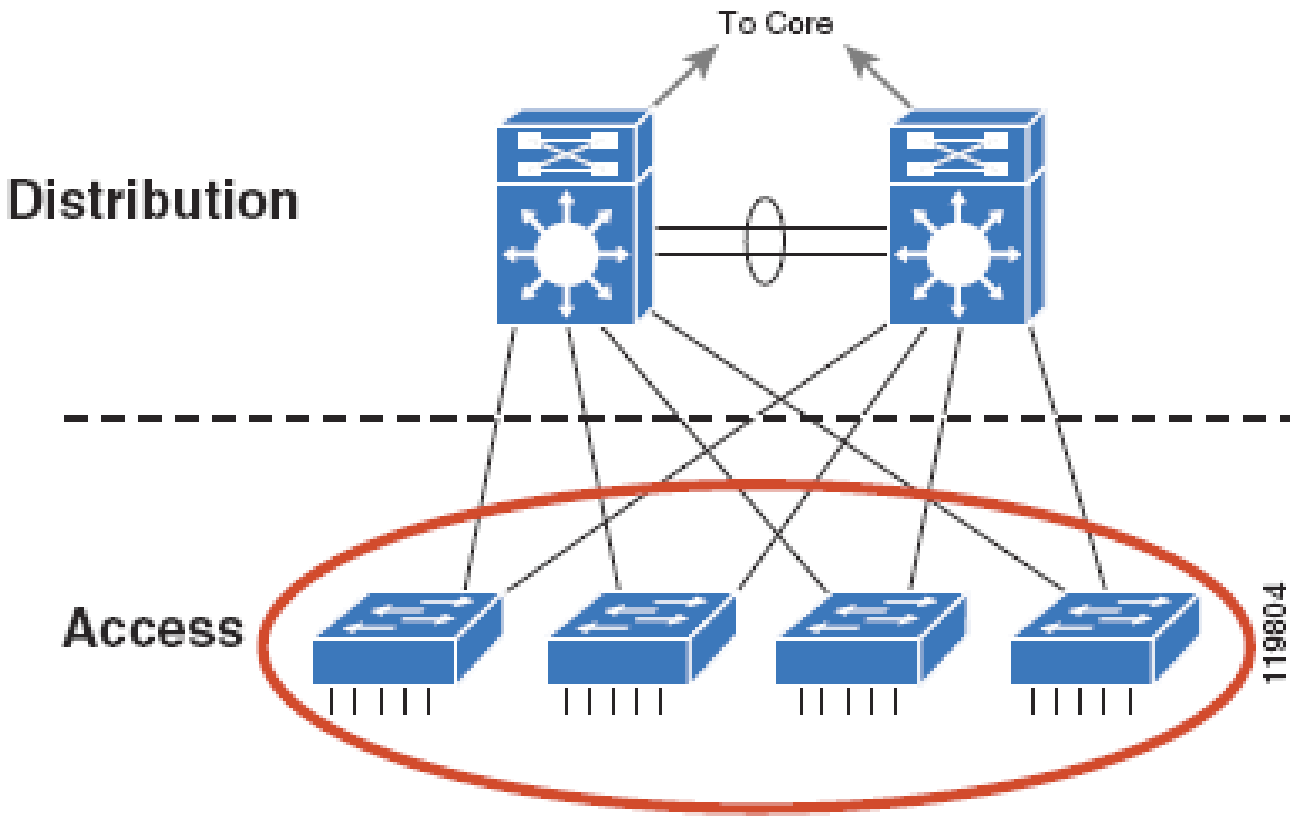
The Layers


Servers
Servers Connected Directly to Distribution
Layer 3 or Layer 2 Switching in Core
Core Layer
Distribution Layer
Access Layer
Layer 3 Switching in Distribution
Layer 3 or Layer 2 Switching in Access
WAN
Internet
PSTN
Workstations

The Modular Approach

- This modular approach has significant benefits including
  - The network is easy to scale
  - The problem domain can be more easily isolated
  - It creates logical interconnection points where protocols changes can occur
  - Failure in any component isolates the devices affected

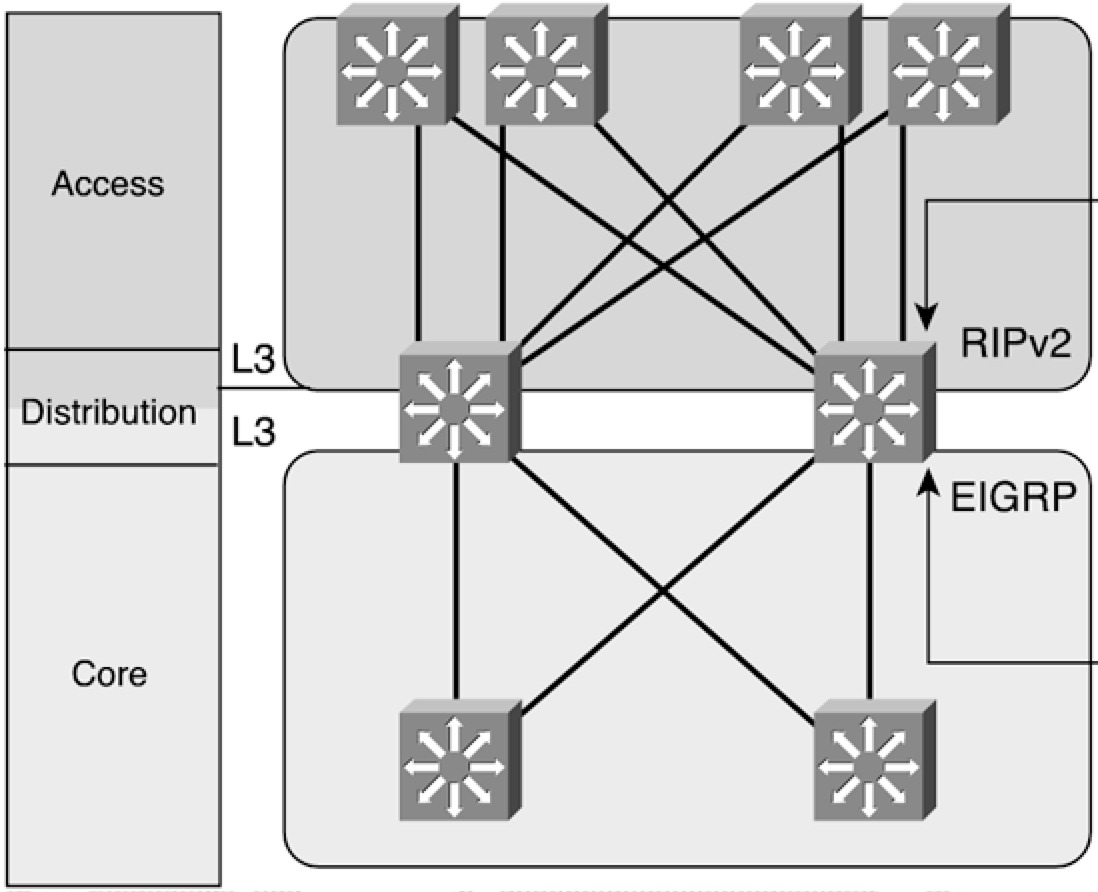
Access Layer



Access Layer

- This level provides local or remote workgroup or user access to the network
- It grants users access to network resources
- Typically this is through a Layer 2 switch
- VLANs may be defined at this layer
- Limit VLANs to a single closet whenever possible

Distribution Layer



L3 Switching in Wiring Closet

Route Filtering Toward the Access Layer

L3 Routing Boundary, Concentration of Access Attachments, Packet Filtering, Policing

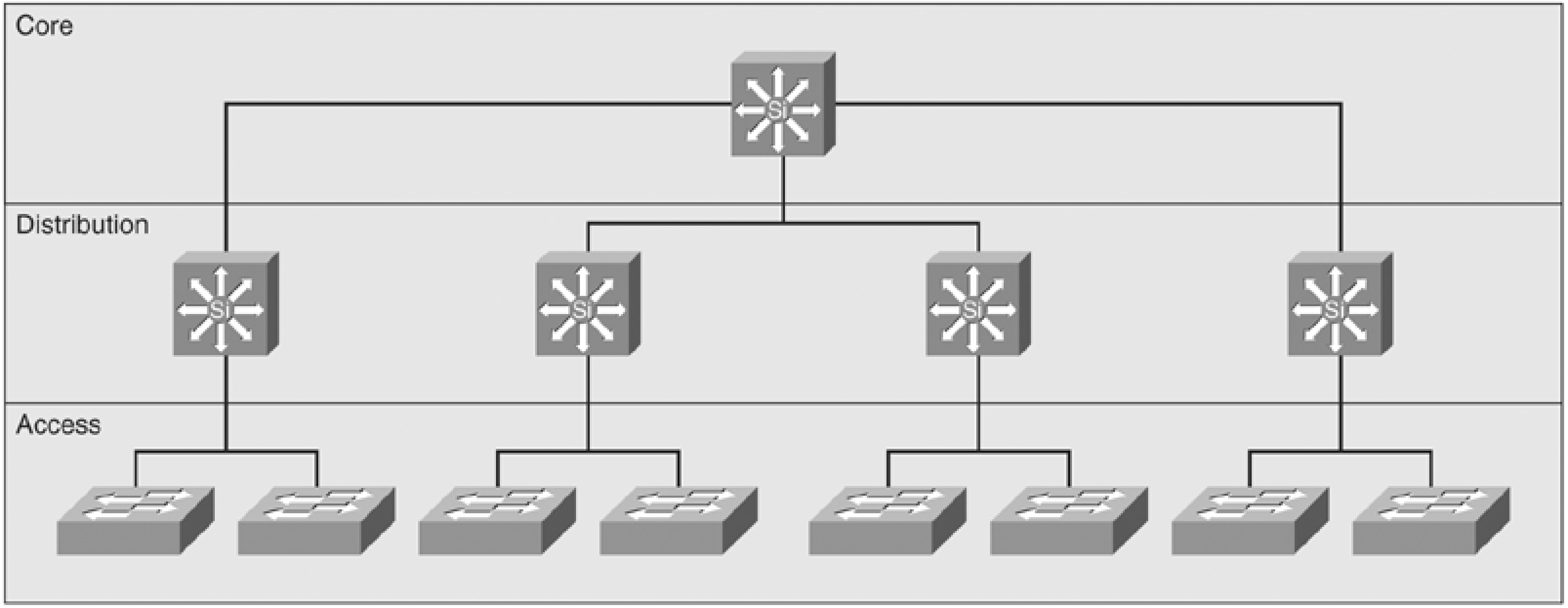
Route Summarization, Eventual Load-Balancing

L3 Switching in Core

Distribution Layer

- The distribution layer devices control access to the shared resources that the network provides
- At the distribution level policy based connectivity issues such as security, traffic loading, and routing occur
- In a small network the access and distribution layers are combined, and there is no core layer

Core Layer



Core Layer

- For large networks the core level provides high speed transport between different parts of the network that have been subdivided at the distribution level as the network has grown in size
- The core layer provides a high speed backbone that should be designed to switch packets as quickly as possible

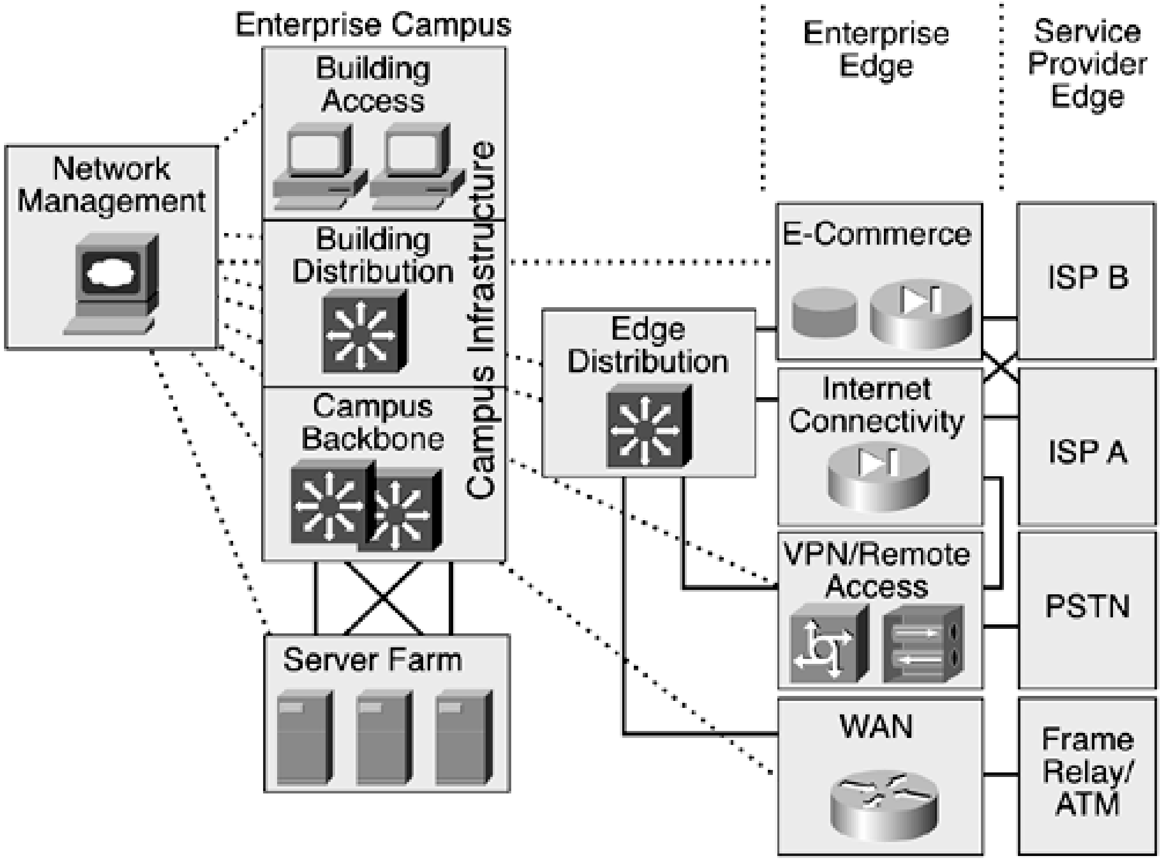
Use of These Layers

- **<u>None of the layers are required for a network except the access layer</u>**
- In many small and medium size networks the access layer is the only one present

Enterprise Composite Model

- A revision and extension to this model is the **Enterprise Composite Network Model**
- This models adds further physical, logical, and functional boundaries to help in scaling the basic hierarchal model
- This model exists within the overall framework of the SONA (Service Oriented Network Architecture) approach discussed below

Enterprise Composite Model



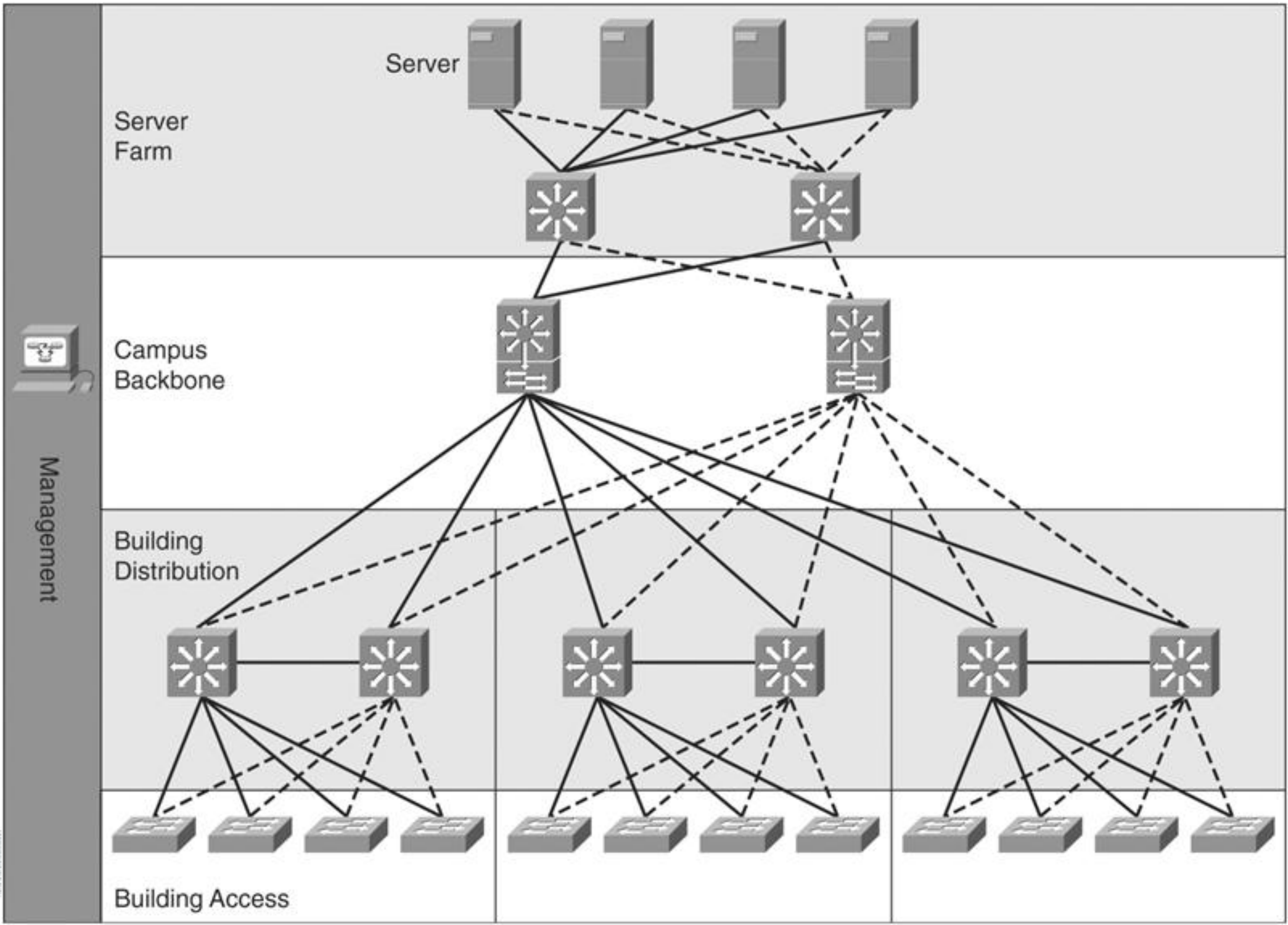
Enterprise Composite Model

- In this approach the access, distribution, and core hierarchy is applied to the various modules as required
- The enterprise composite model is broken up into three large pieces
  - – Enterprise campus
  - – Enterprise edge
  - – Service provider edge

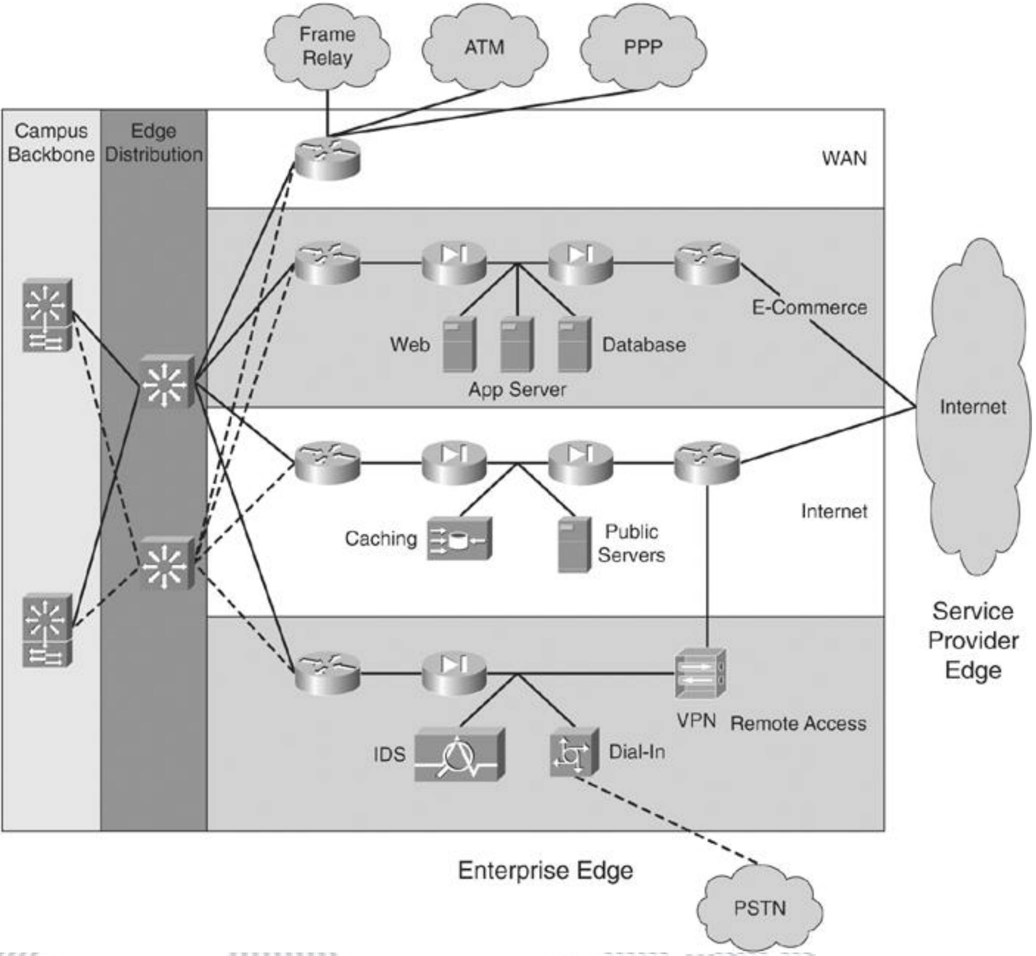
Enterprise Composite Model

- By using this concept a deterministic network with clearly defined boundaries between modules is created
- The model has clear demarcation points
- The network designer knows exactly what traffic is allowed into and out of these demarcation points

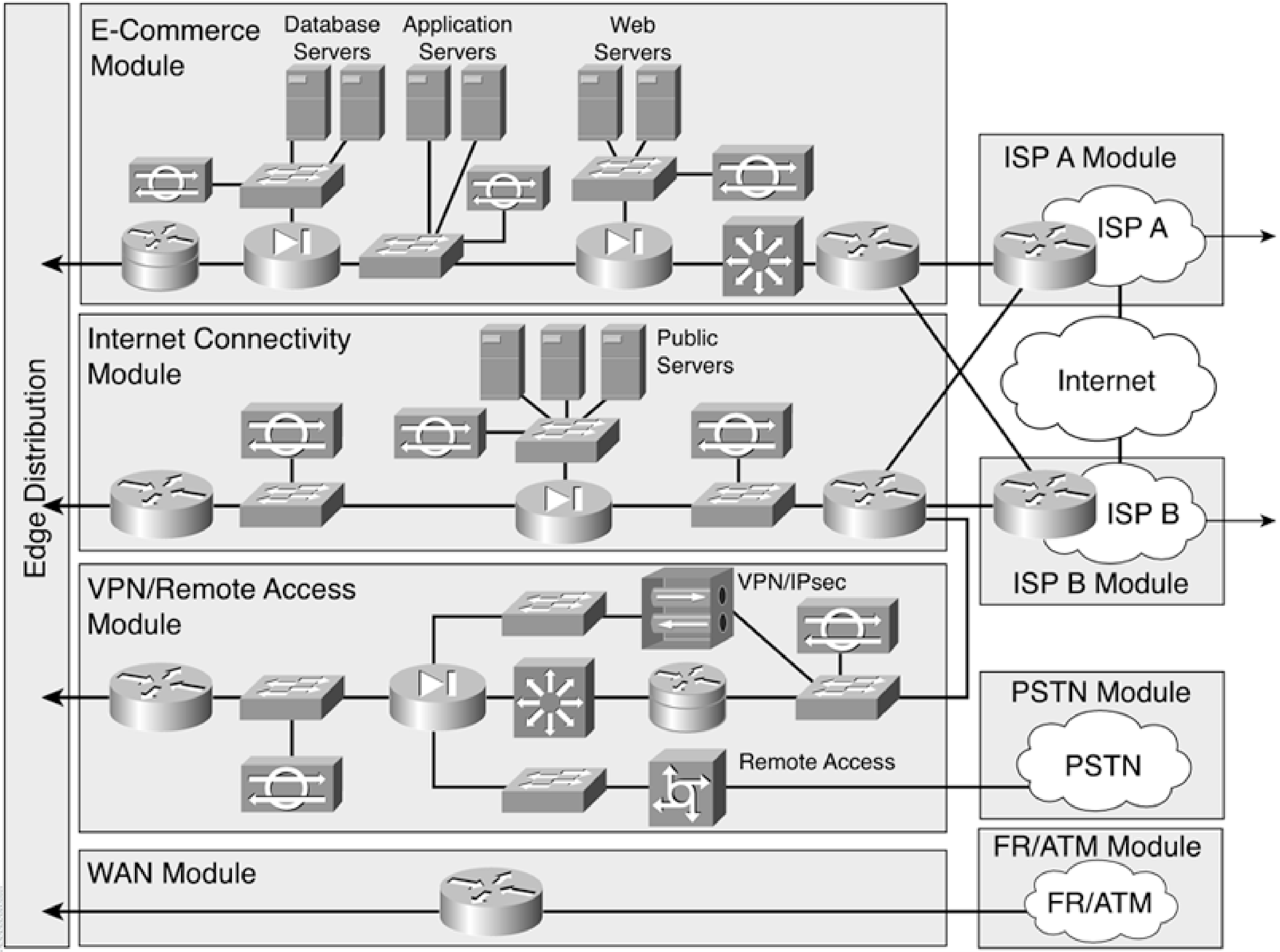
Enterprise Campus



Enterprise Edge



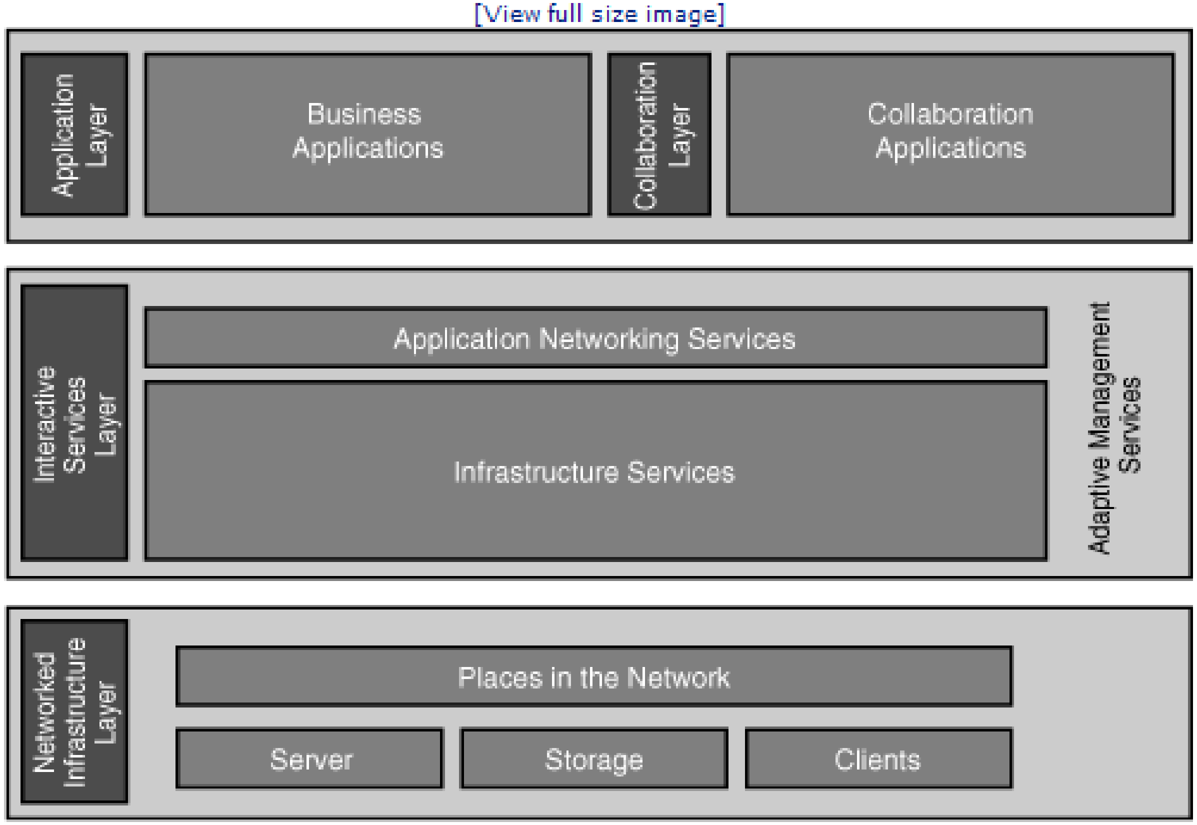
Enterprise Edge



SONA

Figure 2-3. Cisco SONA Framework

[View full size image]


Application Layer
Business Applications
Collaboration Layer
Collaboration Applications
Interactive Services Layer
Application Networking Services
Infrastructure Services
Adaptive Management Services
Networked Infrastructure Layer
Places in the Network
Server
Storage
Clients

SONA

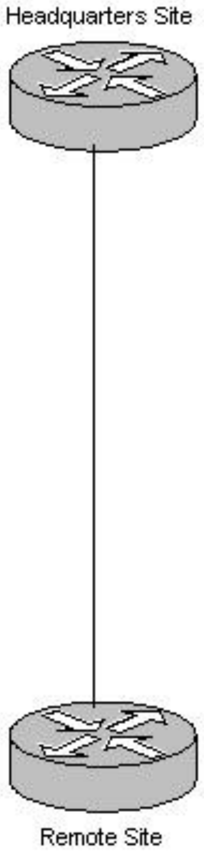
- On top of the traditional access-distribution-core layers and the new Enterprise Composite Model Cisco has overlaid this with the SONA concept
- The basic idea behind SONA is to connect the hardware to the software, as well as the use of these two to deliver a business solution
- In this model there are three basic layers

Physical Network Design

Decide on the Basic Layout

- Let’s also review the layouts that can be used for a network
- In this example as used at the core level
  - – Point-to-Point
  - – Hub and Spoke
  - – Partial mesh
  - – Full mesh

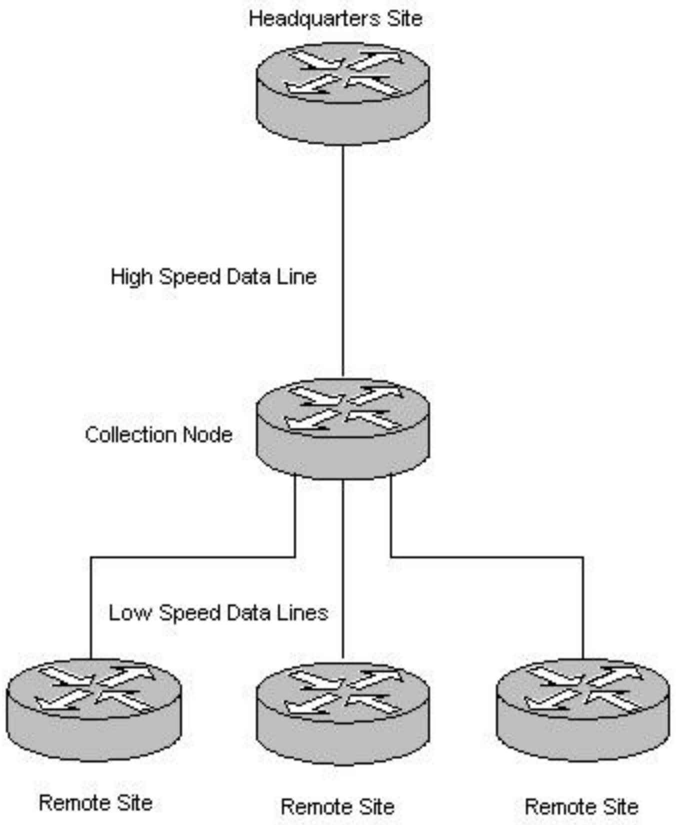
Point-to-Point



Point-to-Point

- A point-to-point design is all that is needed if only two sites are to be connected

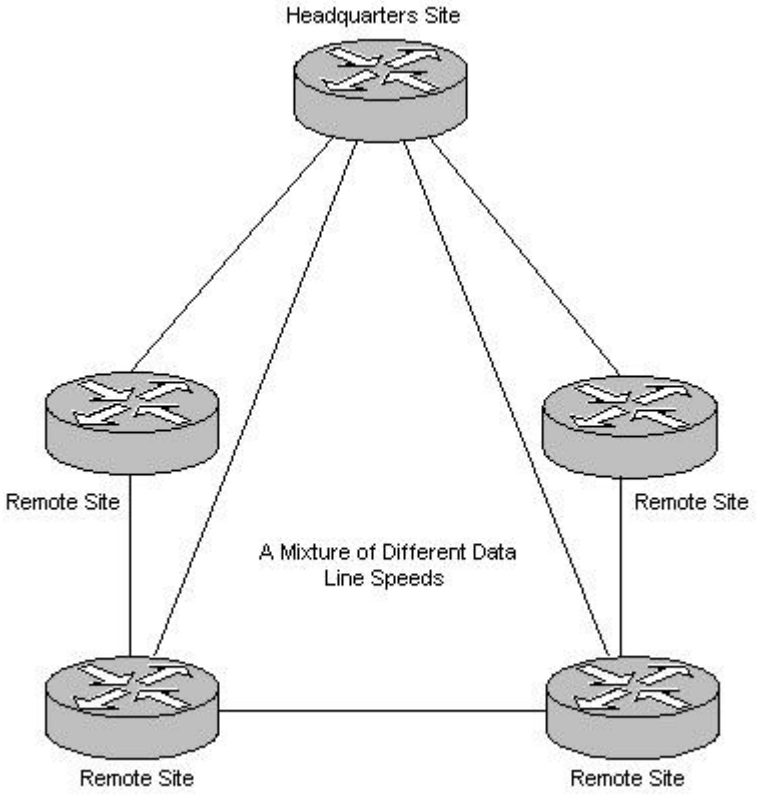
Hub and Spoke



Hub and Spoke

- For a multiple site design the hub and spoke is the least expensive option
- But is has no redundancy
  - If the line to a site goes down, there is no way around it
  - If the line to the collection node or headquarters fails nothing can happen since in this type of arrangement all traffic typically goes all the way to the top before coming back down

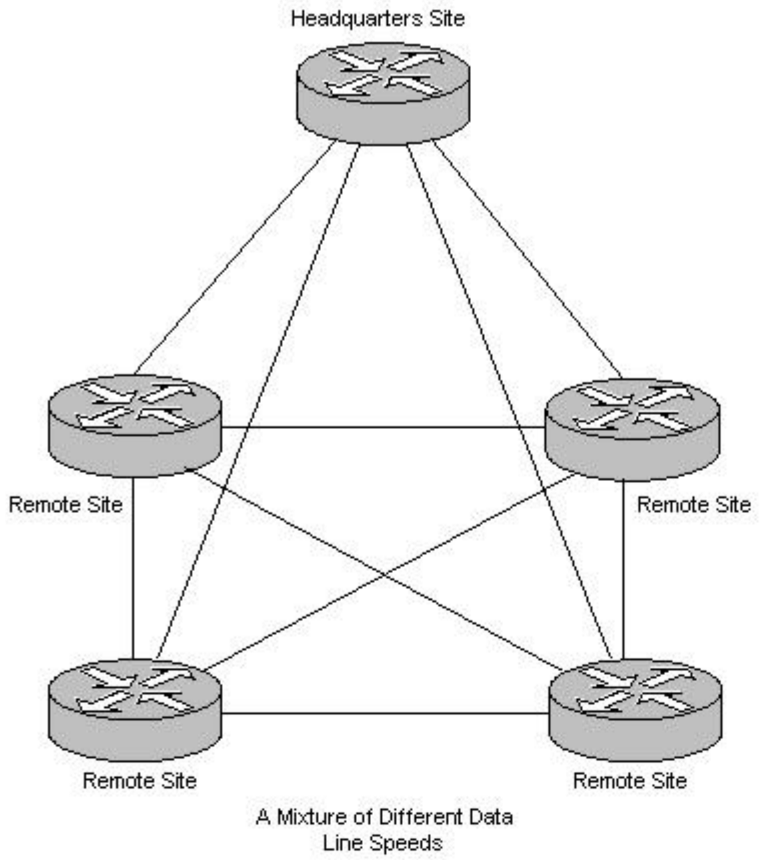
Partial Mesh



Partial Mesh

- Redundancy can be added at some additional cost by using a partial mesh design

Full Mesh


Headquarters Site
Remote Site
Remote Site
Remote Site
Remote Site
A Mixture of Different Data Line Speeds

Full Mesh

- For maximum redundancy a full mesh is used
- This also generates the maximum cost
- Use this formula to determine the number of links required
  - (N*(N-1)/2
    - Where N is the number of connection devices like routers or switches

General Rules

- **General rules for network design include**
  - If a problem is protocol related such as broadcasts or service advertisements
    - Then use routers or layer 3 switches to divide the network
  - If the problem is media contention
    - Replace hubs with switches
  - If the problem is bandwidth
    - Uses higher speed technologies
      - Fast Ethernet/Gigabit Ethernet/ATM

Addressing and Naming

- For a network to scale properly a plan for addressing and naming must be developed
- IP addressing should follow along with the number of discrete networks that will ultimately be needed
- Names should reflect the type of device and location as this will help in troubleshooting

Protocols

- At least at the LAN level, there is no decision anymore: Ethernet is the only choice
- At this level switches are the only choice for a new network
- **There is no reason to use a hub anymore**

Protocols

- At the CAN level for short distances under 500 meters or so there is no decision anymore either
  - – Ethernet is again the only choice
  - – At this level we use layer 2 and layer 3 switches with MMF ports

Protocols

- At the MAN level several technologies are used - such as Ethernet, ATM, and SONET - depending on the distance, budget, and experience and training level of the technical staff
  - **The current trend is to move Any-Over-Ethernet**

Protocols

- At the WAN level there are decisions to be made concerning routing protocols at least
- Routing Protocols are used by routers to learn how to reach other networks
- Which to use depends on
  - Network size
  - Equipment manufacturer
  - Equipment age

Routing Protocols

- Available routing Protocol include
  - Distance Vector
    - RIP
    - EIGRP
  - Link State
    - OSPF
    - IS-IS
  - Path Vector
    - BGP

Network Security Strategies

- The next step is to examine the security needs of the network
- Security must pay attention to
  - Assets to protect
  - Risks to these assets
  - Establishing a clear and enforceable security policy
  - User community training

Network Security Strategies

- Security is implemented through
  - Authentication
  - Authorization
  - Auditing
  - Encryption
  - Connection Control
  - Physical Protection

Network Management

- Management of the network is another consideration to build in
- Management requires timely information
  - Performance
    - Utilization
    - Delay
    - Downtime
    - Throughput
  - Error rates

Technologies and Devices

- We now know what the network will look like
- We know what capabilities the networks needs, such as security and management
- We are now ready to start picking out the bits and pieces to buy
- Here are some guidelines to follow for each type of network

Technologies and Devices

- At the LAN level
  - For cabling use
    - Copper UTP rated for Category 5E, 6, or 6A unless there is a good reason not to
  - To future proof the network
    - Use 6 or 6A instead of 5E
  - In special cases
    - Use MMF for bandwidth intensive applications
    - Or install fiber along with the copper

Technologies and Devices

- At the LAN level also
  - The speed to the desktop should be at least 100 Mbps
  - The connection device to the desktop should be a layer 2 switches

Technologies and Devices

- For a CAN
  - For cabling use
    - Use SMF
    - Unless unusual circumstances occur and cable cannot be run, then use a wireless method
  - To future proof
    - Run cable that contains both MMF and SMF
  - The speed should be whatever is required based on traffic expected
    - Maybe using multiple connections for load balancing

Technologies and Devices

- The connection devices should be Ethernet layer 3 switches in most cases
- ATM is also a possibility (but least likely, its considered legacy)

Technologies and Devices

- For a MAN you may control things from end to end, if the organization is large enough
- More likely you will need to call on an outside supplier for at least the physical links, such as dark fiber between sites
- If you select the cabling, the only thing to use is SMF
- Wireless using RF is an option

Technologies and Devices

- Connection to this fiber can be by
  - – SONET
  - – ATM
  - – Ethernet
  - – A WAN method

Technologies and Devices

- For a WAN as you no longer can control it from end to end, you must rely on someone else
- For the access method most still use Frame Relay or T Carrier (Legacy)
- But DSL and VPNs of all types are getting more an more attention, despite the reliability and latency problems

Technologies and Devices

- The basic decision points for a WAN are
  - Cost of the service
  - Services and technologies offered at the locations
  - Reliability
  - Performance
  - Security
  - Technical support offered

Technologies and Devices

- When selecting the technologies and devices to be used in a CAN, MAN, or WAN link keep in mind that decisions must be made as to what will be used at all seven layers of the OSI model
- All of the functions defined by the model must be accounted for
- Let’s start at the top as this is easy these days

Technologies and Devices

- For layer 7 down to 3, TCP/IP should be used
- Then jump down to layer 1
- What will be used at layer 1 is mostly determined by what is available
- For example, you may wish to use a low cost DSL line, but you may only have access to an ISDN connection at the location

Technologies and Devices

- Once the layer 1 decision is made, this will limit you to what layer 2 encapsulation methods are available for that layer 1 technology

Testing Optimizing Documenting

Testing the Network Design

- A network is too expensive to just put in place without some prototyping and testing before hand, especially in the CAN, MAN, and WAN areas
- Try to get the vendors of the products to setup a test of the proposed solution
- If not, do what can be done in the test lab
- Use modeling tools such as Opnet

Testing the Network Design

- Deploy out to just a few limited sites at first
- Rely on trade publications for results of tests and surveys on the hardware and service providers

Testing the Network Design

- Areas to look at in the test phase include
  - Verify the design meets the business and technical goals
  - Validate the design selections
  - Identify bottlenecks
  - Test redundant channels
  - Assess the impact of total network failure
  - Identify anything that might impede full deployment

Testing the Network Design

- Performance
  - Test the application with transaction volume that is within and at the top of the range expected from the business requirements
  - Make sure that the resulting system behavior is within expectations or any formal service level agreements

Testing the Network Design

- Stress
  - – Expose the system to transaction volume substantially higher than what would normally be expected and over a concentrated time period
- Failure
  - – Regression tests look to see what no longer works when the new stuff goes on line

Testing the Network Design

- Security
  - Ensure that people have the access level that is required and no more and that unauthorized people cannot access the system
- Requirements
  - Track each business requirement through the development process and make sure that it is included in the final system

Testing the Network Design

- Usability
  - Determine that people can use the system easily and without frustration
- Documentation
  - Check that hard-copy and online documentation are understandable and accurate

Testing the Network Design

- Training
  - – Ensure that online or in-person training is effective and meets the training requirements
- Interface
  - – Test your application interfaces with external databases or third-party companies

Testing the Network Design

- Disaster Recovery
  - See whether you can recover the system from a simulated disaster
- Multiple Locations
  - Verify your system can function between multiple locations, if necessary

Optimizing the Network Design

- Once the network is in place and running, it should be optimized
- Exactly how to do this will depend on the hardware and protocols used, so it will not be discussed here in detail

Assessing the Design

- Once the network is designed or when revisiting a network to asses if it needs alterations.

Documenting the Design

- At this stage in the book Oppenheimer discusses how and what to present to management in support of the network design
- Refer to the Top Down Network Design book for the details on this as it is not a subject covered here

Do It All Over Again

- The final step in network design is to do it all over again
- Well not immediately, but on a consistent schedule
- There is a life cycle to a network design plan just as there is for anything
- Oppenheimer uses the Cisco PDIOO – Plan Design Implement Operate Optimize model to illustrate this

PDIOO Process

	Step
↑	Plan
	Design
	Implement
	Operate
	Optimize
	Retire

Network Design Life Cycle

- The idea here is to make this an ongoing process
- Oppenheimer has added a last step to the basic PDIOO model
- This is retirement
- At some point some devices need to be abandoned
- For example a network I worked on was once entirely based on Token Ring LAN devices

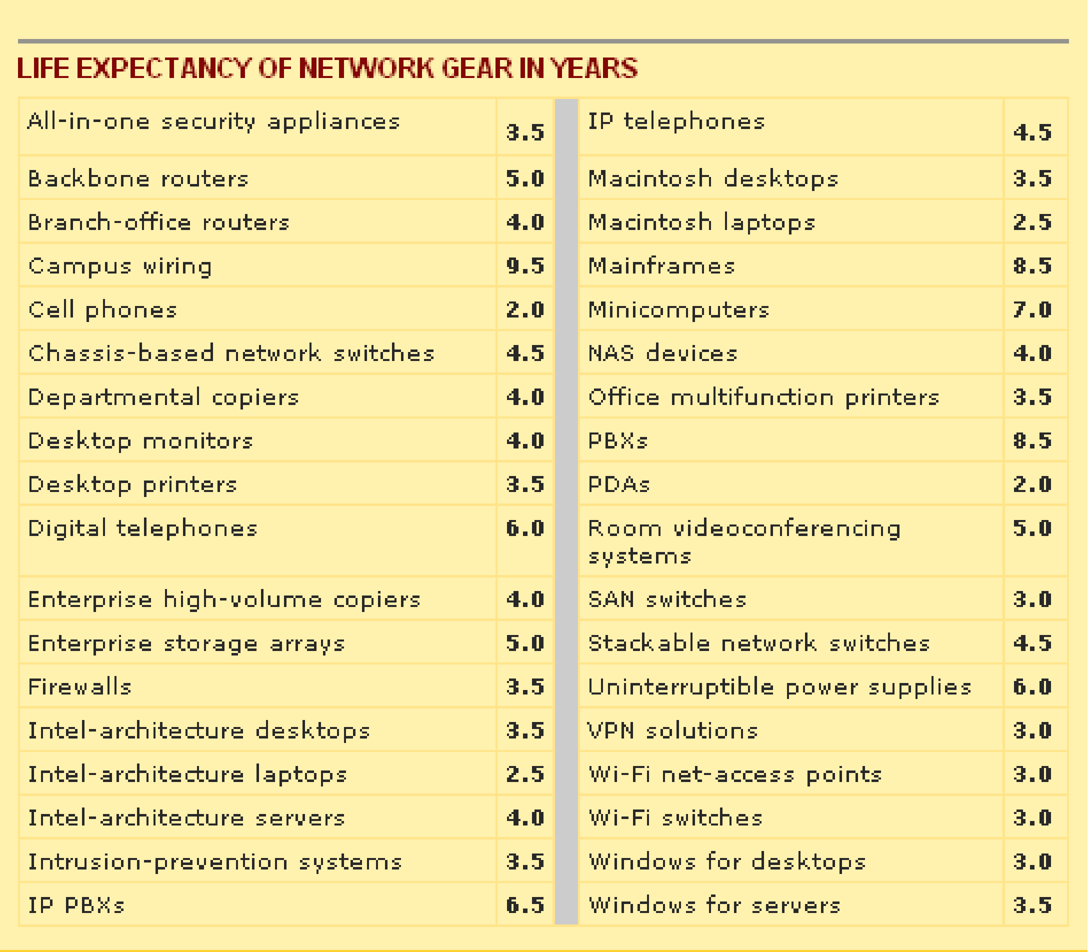
Network Design Life Cycle

- Although these still worked, carried the load placed on it, and for which we had many replacement parts it was time to retire it
- We began a process of slowly converting each site to Ethernet

Equipment Life Cycles

- Network World published an article on guidelines provided by one of their advisory boards on when to upgrade certain devices
- This information will help in the design process so you will know how long things should last
- Here is the summary chart they provided

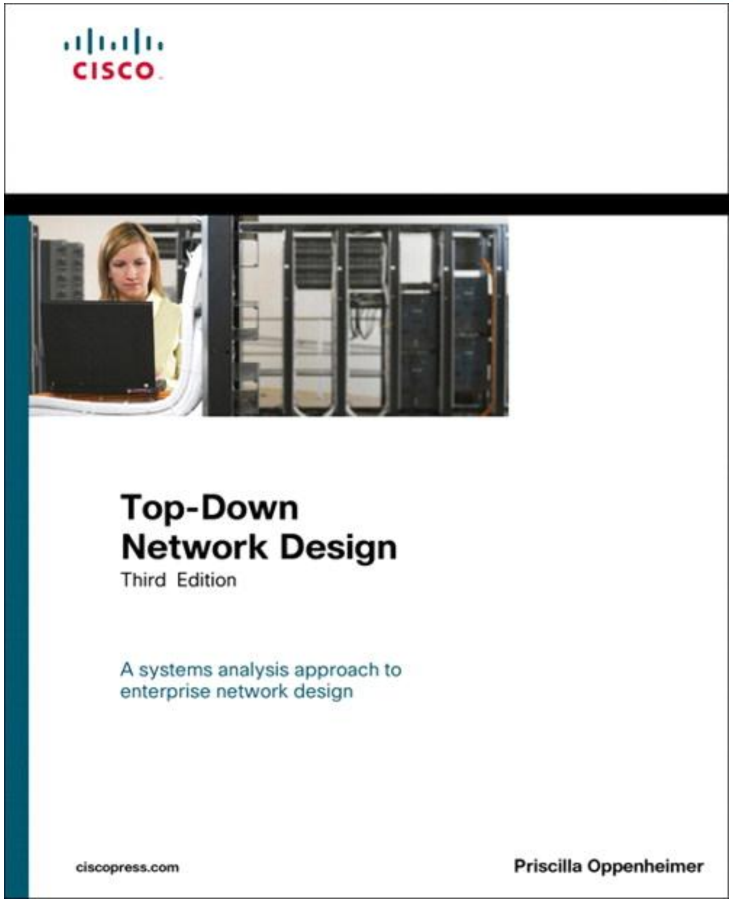
Equipment Life Cycles



LIFE EXPECTANCY OF NETWORK GEAR IN YEARS

All-in-one security appliances	3.5	IP telephones	4.5
Backbone routers	5.0	Macintosh desktops	3.5
Branch-office routers	4.0	Macintosh laptops	2.5
Campus wiring	9.5	Mainframes	8.5
Cell phones	2.0	Minicomputers	7.0
Chassis-based network switches	4.5	NAS devices	4.0
Departmental copiers	4.0	Office multifunction printers	3.5
Desktop monitors	4.0	PBXs	8.5
Desktop printers	3.5	PDAs	2.0
Digital telephones	6.0	Room videoconferencing systems	5.0
Enterprise high-volume copiers	4.0	SAN switches	3.0
Enterprise storage arrays	5.0	Stackable network switches	4.5
Firewalls	3.5	Uninterruptible power supplies	6.0
Intel-architecture desktops	3.5	VPN solutions	3.0
Intel-architecture laptops	2.5	Wi-Fi net-access points	3.0
Intel-architecture servers	4.0	Wi-Fi switches	3.0
Intrusion-prevention systems	3.5	Windows for desktops	3.0
IP PBXs	6.5	Windows for servers	3.5

For More Information



CISCO

Top-Down
Network Design
Third Edition

A systems analysis approach to
enterprise network design

ciscopress.com

Priscilla Oppenheimer

- Top Down Network Design – Third Edition
  - Priscilla Oppenheimer
  - ISBN-10: 1-58720-283-2
  - ISBN-13: 978-1-58720-283-4

Netxar’s Footprint and Overview

Offices

Puerto Rico
San Juan

Republica Dominicana
Santo Domingo

Jamaica
Kingston

Barbados
Bridgetown

Trinidad and Tobago
Port Spain

Who We Are?

Founded on June 2000 in New Hampshire USA. In April 2001, Netxar Headquarters transferred to Puerto Rico to attend the Caribbean region. Our expansion in the region currently includes fully operational offices at Puerto Rico, Dominican Republic and Trinidad & Tobago.

People and Capabilities

- Vast Expertise in the field
- Consultant Focus
- Unified Communication Competencies and operational Experience
- Highest Certification including CCIE, CCNP, CCNA

Services

- Consulting
- Design
- Maintenance & Support
- Managed Services
- Project Management

Technologies

- Advanced Networking
- Unified Communication
- IP Contact Center
- Business Video
- Datacenter and Cloud
- Security
- Wireless