

Chapter 4 **Enterprise Network Design**

Topics covered:

Enterprise Network Design Model. Backbone design concepts. Network security and firewalls. Structured cabling systems. Case studies.

Definition

An enterprise network consists of a group of local area networks (LANs) interconnected using wide area networks (WANs). An enterprise network contains a number of internetworking devices (e.g., switches, routers, gateways, etc) and is under the control of one big organization.

4.1 Enterprise Network Design Model (Hierarchical Model)

There really is no “one size fits all” when it comes to network design.

Two design options:

- Design a network infrastructure from the ground up.
- Meld the new technologies into an existing infrastructure.

A model is vital for analyzing large, complex internetworks.

→ Use of guidelines or rules.

Internetworks are generally implemented in a hierarchical manner.

4.1.1 Three-tier hierarchical model

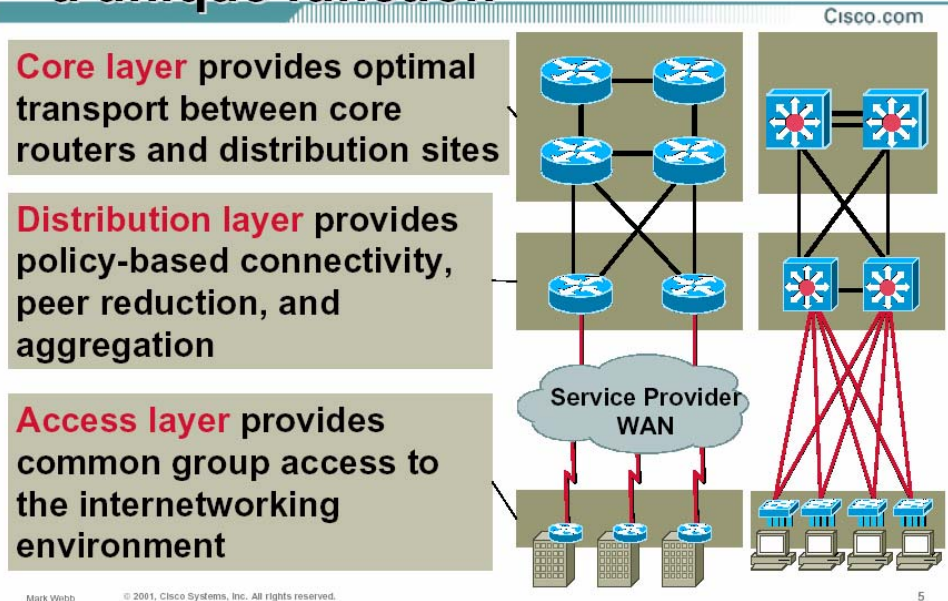
It consists of:

-
-
-

Each level provides a backbone for the level below.

Definition: A backbone is a network whose primary purpose is the interconnection of other networks.

Hierarchy: Each Layer Provides a unique function



(Slide taken from http://www.cisco.com/warp/public/cc/so/neso/meso/uentd_pg.pdf)

4.1.1.1 Core tier

- Provides optimal wide-area transport between geographically remote sites.
- Connects campus networks in a corporate or enterprise WAN
- Services are typically leased from a telecom service provider
- May use the public Internet as enterprise backbone.
- Focus on redundancy and reliability → Continue to function with circuit outages.
- Need to efficiently use bandwidth because of provider tariffs.
- End Stations should not be put in the core

Design Rule:

4.1.1.2 Distribution tier

- Connects multiple networks (departments) within a campus network environment (one or more buildings).
- Includes campus backbone network, based on FDDI, Fast Ethernet, Gigabit Ethernet, or ATM.
- Acts as a concentrator points for many of its access tier sites.
- Links usually owned and/or controlled by the organization.
- Network policy is often implemented in this tier. E.g., security, firewall, encryption, address translation.
 - Network naming and numbering conventions
 - Network security for access to services (admin privileges, etc)
 - Network security for traffic patterns through definition of path metrics (priority, preference, trust, etc)
 - Address aggregation

Design Rule:

4.1.1.3 Access tier

- Usually a LAN or a group of LANs.
- Typically uses Ethernet, Token Ring, or FDDI.
- Can be divided into two levels (workgroup level & desktop level)
 - Workgroup level: e.g., departmental level
 - Desktop level: where end-user devices are attached.
- Where hosts are attached to the network (e.g., labs)
- Connects workgroups (e.g., marketing, administration)
- Usually within a single building (or single floor)
- Provides logical network segmentation, traffic isolation and distributed environment
- Remote (dialup) users are connected at this tier.

Design Rule:

4.1.2 Benefits of a Hierarchical Design Model

Network designs can be: mesh or hierarchical. In a mesh structure, the network topology is flat.

A hierarchical design model has the following advantages:

1. Scalability
 - Design rule: Build hierarchical networks for maximum scalability.
2. Ease of implementation
 - Phased approach is more effective due to cost of resources → efficient allocation of resources in each phase of network deployment.
3. Ease of troubleshooting
 - Easy to isolate problems in the network
 - Use “divide-and-conquer” approach → Temporarily segment the network.
 - Does not affect core tier network
4. Predictability
 - Makes capacity planning for growth easier.
5. Protocol support
 - Mixing new protocol is easier.
 - Merger of companies using different protocol is easier
6. Manageability
 - Easy to implement network management instrumentation by placing probes at different levels of hierarchy

4.1.3 Variations on the three-tier model

4.1.3.1 One-tier Design – Distributed

- Remote networks connect to a pseudo-core

- Good for small networks with no centralized server location.

Advantage: Faster overall response time between peers, simplicity, and cost effectiveness.

Disadvantage: Loss of centralized management control and higher management cost because of duplicated management functions (Responsibilities such as server backups and network documentation are delegated to the access site).

4.1.3.2 One-tier Design – Hub and Spoke

- Servers are located in central farms.

Advantage: Increased management control (centralized).

Disadvantage: Single points of failure and bandwidth aggregation.

4.1.3.3 Two-tier Design

- A campus backbone interconnects separate buildings
 - VLANs can be used to create separate logical networks (i.e., broadcast domains).

4.1.3.4 Redundant Two-tier Hierarchy

- Core LAN backbone is duplicated for total redundancy → more reliable.

4.1.4 Hierarchical Design Guidelines

- Choose a hierarchical model that best fits your requirements
- Do not always completely mesh all tiers of the network (use the backbone for connections).
 - Core connectivity, however, will generally be meshed for circuit redundancy and network convergence speed.
- Do not place end stations on backbones → Improves the reliability of the backbone.
- Workgroup LANs should keep as much as 80% of their traffic local to the workgroup →

- Use specific features at the appropriate hierarchical level.
- Control the diameter of a hierarchical enterprise network topology (in most cases, 3 major layers are sufficient)
 - Provides low and predictable latency.
 - Helps predict routing paths, traffic flows, & capacity requirements.
 - Makes troubleshooting & network documentation easier.
- Avoid chains at the access layer (e.g., connecting a branch network to another branch, adding a 4th layer)

- Avoid backdoors (i.e., connection between devices in the same layer)
 - Cause unexpected routing problems
 - Make network documentation and troubleshooting more difficult

- Design the access layer first, then the distribution layer, and finally the core layer.
 - Helps, more accurately, perform capacity planning at the distribution and core layers.

4.1.5 Mesh vs. Hierarchical-Mesh Topologies

- In full-mesh topology, every router or switch is connected to every other router or switch. It provides complete redundancy. → Offers good performance.
 - Number of links in this topology is:

- A partial-mesh topology has fewer connections (To reach another router, the network might require traversing intermediate links).

- Mesh networks can be expensive to deploy and maintain
 - Especially full-mesh networks

 - Hard to optimize, troubleshoot, and upgrade

 - Have scalability limits for groups of routers that broadcast routing updates (processing increases)

- A classic hierarchical and redundant enterprise design uses a partial-mesh hierarchy rather than a full mesh.

4.2 Redundant Network Design Topologies

Redundancy:

- Provides network availability by duplicating network links and interconnectivity devices
- Eliminates the possibility of having single point of failure on the network

Goal:

- Helps you meet the availability goals for users accessing local services (in campus networks)
- Helps you meet overall availability and performance goals (in enterprise networks)
- Adds complexity to the network topology and to network addressing and routing

Note:

4.2.1 Backup Paths

- A backup path:
 - Consists of routers and switches and individual backup links between routers and switches that duplicate devices and links on the primary path.
 - Maintains interconnectivity even when one or more links are down
- Two aspects of the backup path to consider:
 - How much capacity does the backup path support?
 - How quickly will the network begin to use the backup path?

- Use a modeling tool to predict network performance when backup is in use:
 - It can be acceptable that the performance of the backup path is worse than that of the primary path.
- Backup path usually have less capacity than primary path, e.g., a leased line with a backup dial-up line. However, requirements may state that both must provide the same performance → this is expensive → Tradeoff: Cost vs. Reliability.
- Automatic fail-over is necessary for mission-critical applications.
 - Where disruption is not acceptable.
 - If manual reconfiguration is required to switch to a backup path, users will notice disruption.
 - Redundant, partial mesh network design speeds automatic recovery time when a link fails, e.g., spanning tree.
- Backup path must be tested
 - Do not wait for a catastrophe to happen.
- Some backup links are used for load balancing as well as redundancy
 - Advantage:

4.2.2 Load Balancing

- Redundancy improves performance by supporting load balancing across parallel links.
- Load balancing must be planned and in some cases configured.
 - However, some protocols do not support load balancing by default.
- Some internetworking devices support balancing across multiple parallel paths.

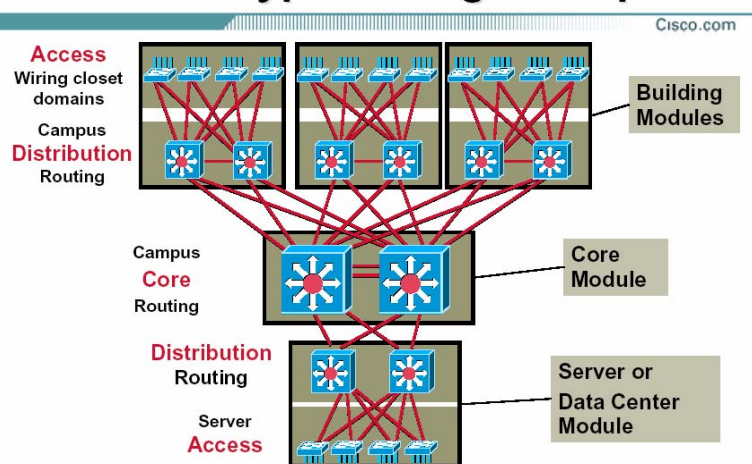
4.3 Designing a Campus Network Design Topology

- Redundant LAN segments
 - Design redundant links between LAN switches.
 - The spanning tree algorithm guarantees that only one path is active between two stations → Good solution for redundancy, but not for load balancing.

- Cisco switches let you implement one spanning tree per VLAN. Redundant links can offer load balancing and fault tolerance.

- Server redundancy
 - Depends on the customer's requirements
 - Services include: file, web, DHCP (Dynamic Host Configuration Protocol), name, database.
 - Use redundant servers when needed (e.g., DHCP). The servers should hold redundant (mirrored) copies of the DHCP database. DHCP servers can be placed at either the access or distribution layer.

Structure: Typical Large Campus



4.4 Designing an Enterprise Network Design Topology

- Enterprise network design topology should meet a customer's goals for availability and performance by featuring:
 - Redundant LAN and WAN segments in the intranet
 - Multiple paths to extranets and the Internet.
 - Extranet: an internal internetwork that is accessible by outside parties, e.g., suppliers, resellers, etc.
- Redundant WAN segments
 - Usually uses a hierarchical partial-mesh topology.
 - **Circuit diversity:** physical circuit routing of backup WAN links and primary WAN links should be different than each other.
 - **Multihoming** the Internet connection: provides an enterprise network more than one entry into the Internet (i.e., redundancy and fault tolerance)
 - **Definition: *Multihoming*** - provide more than one connection for a system to access and offer network services
 - Example: A server is multihomed if it has more than one network-layer address.
 - **Options for multihoming the Internet connection** (i.e., the enterprise network is multihomed to the Internet)

- **Virtual Private Networks (VPNs):** enables the use of a public network, such as the Internet, to provide a secure connection among sites on the organization's internetwork.
 - A public network is used as a backbone for the enterprise network.
 - Links remote offices together.
 - Inexpensive compared to private leased lines.
 - Private data is encrypted for routing through the public network
 - No permanent link is required.
 - Can use Dial-on-demand routing (DDR).

4.5 Secure Network Design Topologies

- Planning for physical security: protection from unauthorized access, theft, vandalism, and natural disasters (e.g., floods, fires, storms, and earthquakes)
 - Not an aspect of logical network design, but it has an impact on it.
- Meeting security goals with firewall topologies:
 - **Definition: Firewall** – a system or combination of systems that enforces a boundary between two or more networks (according to the National Computer Security Association (NCSA)).
 - A firewall can be:
 - a router with access control lists (ACLs),
 - a dedicated hardware box (e.g., PIX), or
 - a software running on a PC or UNIX system.
 - A firewall should be placed in the network so that all traffic from outside the protected network must pass through the firewall.
 - A firewall is especially important at the boundary between the enterprise network and the Internet.
 - A basic firewall topology is simply a router with:
 - a WAN connection to the Internet,
 - a LAN connection to the enterprise network, and
 - a software that has security feature.
 - Larger companies use a dedicated firewall in addition to a router between the Internet and the enterprise network.
 - Firewall topology can include a public LAN that hosts Web, FTP, DNS, and SMTP servers (for customers who need to publish public data).
 - This public LAN is referred to as: *demilitarized or free-trade zone*.

4.6 Backbone Design

There are two types of backbone design:

- Distributed backbones
- Collapsed backbones

4.6.1 Distributed Backbones

4.6.1.1 Distributed Backbones in Buildings (Figure 5-3 in [1])

- Each floor's router is directly connected to a centralized backbone.
- The backbone is typically an FDDI ring. This provides maximum fault tolerance.
- Generally, do not contain a single point of failure
- Requires extra input and output ports for each component
 - Faults quickly corrected by isolation process
 - High cost
- **Drawbacks:**
 - Multiple IP network numbers → difficult to add, move, or change users.
 - More expensive
 - Migration to switching not easy.
 - Less-flexible approach to wiring a building.

4.6.1.2 Distributed Backbones on the Campus (Figure 5-4 in [1])

- More resource-efficient solution than in a building.
- **Drawback:**
 - Lack of flexibility in connecting to other buildings on the campus.

4.6.2 Collapsed Backbones (Figures 5-5 and 5-6 in [1])

- Has a single concentration point connecting all floors.
- All floor-to-floor connectivity passes through the backbone component.
- Problem isolation is simple, while finding problem's root cause is difficult.
- More flexible and cost-effective approach to wiring a building.
- Changes can be easily made.
- Can be extended to accommodate VLANs.
 - VLANs in a building
 - More flexibility in positioning of end stations and servers.
 - VLANs across a campus
 - One switch acts as the backbone for the entire campus.
 - Assign stations to VLANs such that only 20% of their traffic is destined to other VLANs.

- Single point of failure (Router)
 - **Solution:** Router with HSRP (Hot Standby Router Protocol).
 - **HSRP:** Provides a way for an IP workstation to keep communicating on an internetwork even if its default router becomes unavailable.
 - HSRP works by creating a phantom router with its own IP and MAC addresses.
 - Each workstation uses the phantom as its default router.
 - When a workstation broadcasts an ARP frame to find its default router, the active HSRP router responds with the phantom's MAC address.
 - If the active HSRP router goes offline, a standby router takes over as active router.
 - HSRP routers on a LAN communicate to designate an active and standby router.

4.7 Structured cabling Systems (SCS)

4.7.1 SCS Principles

- Studies have shown that more than 50% of all network disruptions are related to cabling.
- IBM & AT&T developed generic cabling systems based on STP cables and UTP cables, respectively.

- SCS objectives:
 - Use a single common cable type that supports many applications
 - Remain cost effective (i.e., minimum additional equipment required)
 - Based on a “flood wiring” approach.
 - To minimize the impact of moves, additions, and changes → minimize the ongoing cost of ownership
 - Ability to support any given application
 - Reliability of the system.
- SCS topology:
 - Based on “star” topology in a tree-like fashion.
- Distribution point provides the administration (patching) points for the system
- All systems must comprise at least the horizontal distribution level
- At each distribution point, application specific equipment (e.g., computer systems, repeaters, switches, etc) are patched into the system for user connectivity.

- SCS standards:
 - EIA/TIA-568 standard: “Commercial Building Telecommunications Wiring Standard” (1990)
 - Included the use of both 10Base2 and 10Base5 media (i.e., coaxial)
 - EIA: Electronics Industry Association (www.eia.org)
 - TIA: Telecommunications Industry Association (www.tiaonline.org)
 - ANSI/EIA/TIA-568-A standard: provides ideal design platform
 - Different media is possible
 - SCS terminology in ANSI is different from ISO’s
 - ANSI: American National Standards Institute
 - ISO: International Standards Organization

4.7.2 Areas within a SCS System

- SCS comprises 3 cabling subsystems:
 - Horizontal cabling subsystem.
 - Building backbone subsystem.
 - Campus backbone subsystem.
- The work area cabling is also necessary but outside the scope of SCS standards.

4.7.2.1 Horizontal Cabling Subsystem

- Includes:
 - Horizontal distribution cables
 - Connecting hardware
 - Cross-connect patching at the Floor Distributor (FD)
- Media options: UTP, STP, optical fiber (multimode)
- Horizontal distribution cable should be continuous wherever possible
 - However, a single transition point can be included between FD and TO, e.g.:
 - Transition between 2 types of cabling
 - Use of 25 pair cables, then 4 pair cable to the TO.
 → Source of increased crosstalk.
- Maximum distance is 90 meters from FD to TO.
 - Maximum 5 meters for patch cords and work area fly leads.
 → Maximum $5+90+5=100$ meters between equipment and end-user.
 (100 meters is the maximum transmission distance for high speed data over twisted pair)

4.7.2.2 Building Backbone Cabling Subsystem

- Includes:
 - Building backbone cable
 - Termination hardware
 - Cross-connect patching at the Building Distributor (BD)
- Media options: UTP, STP, optical fiber (multimode and single mode)
- Transition points not allowed.
- Maximum distance is 500 meters.
- Maximum 20 meters for patch cords length.

4.7.2.3 Campus Backbone Cabling Subsystem

- Includes:
 - Campus backbone cable
 - Mechanical termination of backbone cable
 - Cross-connect patching within the Campus Distributor (CD)
- Media options: mainly optical fiber (for longer distances and electrical isolation)
- Maximum distance is 1500 meters.
 - Added to the building backbone maximum distance (i.e., 500 meters)
→ 2 km, that is the maximum supported distance for high speed data over multimode fiber optic.
- Maximum 20 meters for patch cords length.

4.7.3 Application Classes

- Applications must be taken in consideration when designing an SCS
 - Example:** Ethernet maximum transmission limit is 100 meters over UTP cables.
 - Ethernet will not run over UTP backbone of 500 meters.
 - Backbone should be reduced to 100 meters or media changed to fiber optic
- Mapping of LAN applications onto SCS:
 - Ethernet is the easiest to map onto SCS because standards were written for twisted pair media.

4.7.4 SCS Patching

4.7.4.1 Inter-Connect (Direct) Patching

- Convenient when port presentation is the same on equipment and patch panel (e.g., RJ-45)

- Requires fewer connections.
 - Minimizes the amount of crosstalk
- **Problem:** Patch cables can become a tangled mess with cables going in all directions (bad presentation).

4.7.4.2 Cross-Connect (Indirect) Patching

- Involves the addition of extra patch panels where equipments are permanently terminated.

- Much neater cable presentation.

- **Problem:** More crosstalk on the link mainly if the full bandwidth of the cabling is being pushed to its limits over the maximum 90 meters distribution distance.
 - This can be avoided with good installation practices.

4.7.5 Design Guidelines

- Start from the edge (i.e., work area) and work back to the center.

Example: sizing of work areas, media type of horizontal cabling, location of FD, cabling pathways, etc.

- System administration must start at the planning stage to maximize the potential of the cabling system.

Example: outlet identification, numbering/naming, etc.

4.7.5.1 Work Area

- 1000 m² of floor space is the maximum area to be supported from one FD.
- Work area sizing: 2 m² → 10 m² (However, this is site specific decision)
- Number of TOs per work area: at least 2 (1 copper, and 1 fiber or copper).
- Design work areas to form logical “zones”
 - Some buildings may require multiple FDs to service all locations on a floor.
- Overlaying, or interleaving the cabling (multiple pathways are used) can provide a high degree of resilience when a pathway is damaged.
 - Much higher installation and material cost.

4.7.5.2 Distributor Layout

- Type of patch panel, FD housing (cabinet, rack, etc), sizing, location, etc.
- Each cabinet contains a proportion of all elements (e.g., some horizontal cabling, some equipment, etc.)

Advantage: If a cabinet is lost (e.g., due to power failure), a proportion of users will not be affected.

4.7.5.3 The Backbone

- May need to provide two backbones: one for voice and one for data.
- Resilience: implement multiple backbones via multiple risers and have additional capacity in each backbone.

4.8 References

1. “Cisco Internetwork Design” edited by Matthew H. Birkner. Cisco Systems, 2000
2. “Top-Down Network Design” by Priscilla Oppenheimer, Cisco Press, 2001
3. http://www.cisco.com/warp/public/cc/so/neso/meso/uentd_pg.pdf
4. “The Switch Book” by Rich Seifert. John Wiley & Sons Inc., 2000.
5. “LAN Technologies Explained” by Philip Miller and Michael Cummins. Digital Press, 2000