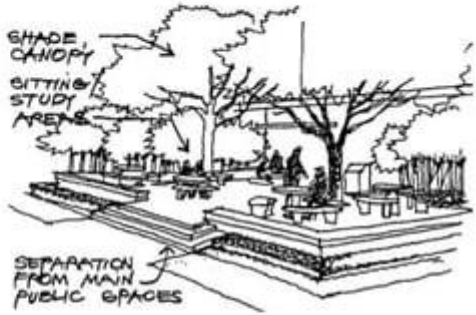
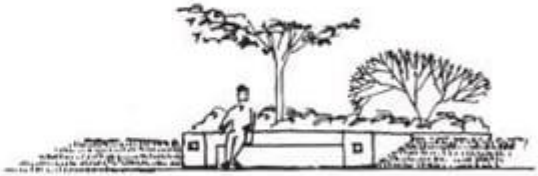
Campus design considerations

DESIGN CONSIDERATIONS

- BUILDING HEARTH
- CLASSROOM DISTRIBUTION
- ENOUGH STORAGE
- FABRIC OF DEPARTMENTS
- FACULTY-STUDENT MIX
- FLEXIBILITY AND LONGEVITY
- NO SIGNS NEEDED
- OFFICE CONNECTIONS
- ORGANIZATIONAL CLARITY
- OUTDOOR CLASSROOM
- PLACES TO WAIT
- POOLS OF LIGHT
- PUBLIC GRADIENT
- QUALITY OF LIGHT
- STUDENT HOUSING
- UNIVERSITY SHAPE AND DIAMETER





Common Campus network Hierarchical Design Models

- A campus network is generally the portion of the network infrastructure that provides access to network communication services and resources to end users and devices that spread over a single geographic location.
- It might be a single floor, a building, or even a group of buildings spread over an extended geographic area.
- Cisco's hierarchical network design model breaks the complex problem of network design into smaller and more manageable.
- Each level, or tier in the hierarchy is focused on specific set of roles. This helps the network designer and architect to optimize and select the right network hardware, software and features to perform specific roles for that network layer.

A typical enterprise hierarchical campus network design includes the following three layers:

- The Core layer that provides optimal transport between sites and high performance routing
- The Distribution layer that provides policy-based connectivity and control boundary between the access and core layers
- The Access layer that provides workgroup/user access to the network

Campus Core Design Considerations

- Low price per port and high port density can govern switch choice for wiring closet environments, but high-performance wire-rate multilayer switching drives the Campus Core design.
- Using Campus Core switches reduces the number of connections between the Building Distribution layer switches and simplifies the integration of the Server Farm module and Enterprise Edge modules.
- Campus Core switches are primarily focused on wire-speed forwarding on all interfaces and are differentiated by the level of performance achieved per port rather than by high port densities.
- Deploy a dedicated Campus Core layer to connect three or more buildings in the Enterprise Campus, or four or more pairs of Building Distribution switches in a very large campus. Campus Core switches are typically multilayer switches.

Issues to consider in a Campus Core layer design

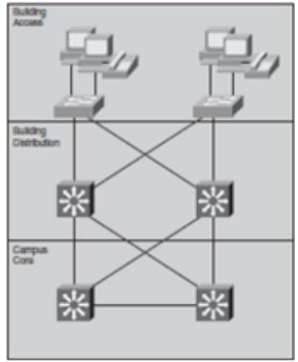
- The performance needed in the Campus Core network.
- The number of high-capacity ports for Building Distribution layer aggregation and connection to the Server Farm module or Enterprise Edge modules.
- High availability and redundancy requirements. To provide adequate redundancy, at least two separate switches (ideally located in different buildings) should be deployed.

Enterprise Edge and WAN connectivity

- For many organizations, the Campus Core provides Enterprise Edge and WAN connectivity through Edge Distribution switches connected to the core.
- For large enterprises with a data center, the Enterprise Edge and WAN connectivity are aggregated at the data center module.
- Typically, the Campus Core switches should deliver high-performance, multilayer switching solutions for the Enterprise Campus and should address requirements for the following:
  - Gigabit density
  - Data and voice integration
  - LAN, WAN, and metropolitan area network (MAN) convergence
  - Scalability
  - High availability
  - Intelligent multilayer switching in the Campus Core, and to the Building Distribution and Server Farm environments.

Large Campus Design

- For a large campus, the most flexible and scalable Campus Core layer consists of dual multilayer switches



Multilayer-switched Campus Core layers features

- **Reduced multilayer switch peering** (routing adjacencies): Each multilayer Building Distribution switch connects to only two multilayer Campus Core switches, using a redundant triangle configuration. This implementation simplifies any-to-any connectivity between Building Distribution and Campus Core switches and is scalable to an arbitrarily large size. It also supports redundancy and load sharing.

- **Topology with no spanning-tree loops**: No STP activity exists in the Campus Core or on the Building Distribution links to the Campus Core layer, because all the links are Layer 3 (routed) links. Arbitrary topologies are supported by the routing protocol used in the Campus Core layer. Because the core is routed, it also provides multicast and broadcast control.

- **Improved network infrastructure services support:** Multilayer Campus Core switches provide better support for intelligent network services than data link layer core switches could support.

Small and Medium Campus Design Options

- A small campus (or large branch) network might have fewer than 200 end devices, and the network servers and workstations might be connected to the same wiring closet.
- Because switches in a small campus network design may not require high-end switching performance or much scaling capability, in many cases, the Campus Core and Building Distribution layers can be combined into a single layer.
- This design can scale to only a few Building Access layer switches.
- A low-end multilayer switch provides routing services closer to the end user when multiple VLANs exist.
- For a very small office, one low-end multilayer switch may support the LAN access requirements for the entire office.

Small and Medium Campus Design Options

- For a medium-sized campus with 200 to 1000 end devices, the network infrastructure typically consists of Building Access layer switches with uplinks to Building Distribution/Campus Core multilayer switches that can support the performance requirements of a medium-sized campus network.
- If redundancy is required, redundant multilayer switches connect to the Building Access switches, providing full link redundancy.

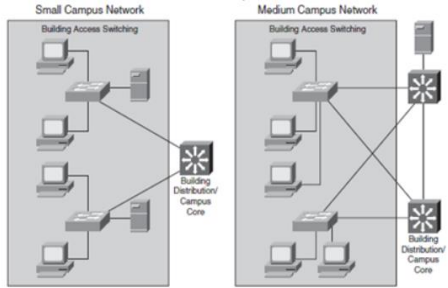
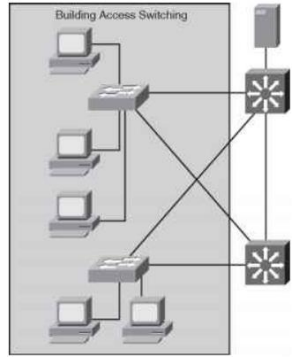


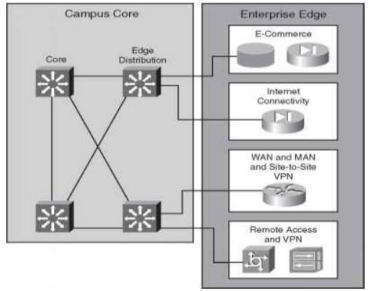
Figure *Small and Medium Campus Design Options*

Building Distribution/ Campus Core

- For a medium-sized campus with 200 to 1000 end devices, the network infrastructure typically consists of Building Access layer switches with uplinks to Building Distribution/Campus Core multilayer switches that can support the performance requirements of a medium-sized campus network. If redundancy is required, redundant multilayer switches connect to the Building Access switches.



Edge Distribution at the Campus Core



- The Edge Distribution multilayer switches filter and route traffic into the Campus Core, aggregate Enterprise Edge connectivity, and provide advanced services.
- The Edge Distribution multilayer switches filter and route traffic into the Campus Core, aggregate Enterprise Edge connectivity, and provide advanced services.
- Switching speed is not as important as security in the Edge Distribution module, which isolates and controls access to devices that are located in the Enterprise Edge modules (for example, servers in an E-commerce module or public servers in an Internet Connectivity module). These servers are closer to the external users and therefore introduce a higher risk to the internal campus.

Edge Distribution at the Campus Core

To protect the Campus Core from threats, the switches in the Edge Distribution module must protect the campus from the following attacks:

- **Unauthorized access**:
  - All connections from the Edge Distribution module that pass through the Campus Core must be verified against the user and the user's rights.
  - Filtering mechanisms must provide granular control over specific edge subnets and their capability to reach areas within the campus.
- **IP spoofing**:
  - IP spoofing is a hacker technique for impersonating the identity of another user by using that user's IP address.
  - Denial of service (DoS) attacks use IP spoofing to generate requests to servers, using the stolen IP address as a source.
  - The server therefore does not respond to the original source, but it does respond to the stolen IP address.
  - A significant amount of this type of traffic causes the attacked server to be unavailable, thereby interrupting business.
  - DoS attacks are a problem because they are difficult to detect and defend against; attackers can use a valid internal IP address for the source address of IP packets that produce the attack.

- **Network reconnaissance**:
  - Network reconnaissance (or discovery) sends packets into the network and collects responses from the network devices.
  - These responses provide basic information about the internal network topology.
  - Network intruders use this approach to find out about network devices and the services that run on them.
  - Therefore, filtering traffic from network reconnaissance mechanisms before it enters the enterprise network can be crucial. Traffic that is not essential must be limited to prevent a hacker from performing network reconnaissance.
- **Packet sniffers**:
  - Packet sniffers are devices that monitor and capture the traffic in the network and might be used by hackers.
  - Packets belonging to the same broadcast domain are vulnerable to capture by packet sniffers, especially if the packets are broadcast or multicast.
  - Because most of the traffic to and from the Edge Distribution module is business-critical, corporations cannot afford this type of security lapse.
  - Multilayer switches can prevent such an occurrence.

Designing a Campus Network Design Topology

- Campus network design topologies should meet a customer's goals for availability and performance by featuring small bandwidth domains, small broadcast domains, redundancy, mirrored servers, and multiple ways for a workstation to reach a router for off-net communications.
- Campus networks should be design using a hierarchical, modular approach so that the network offers good performance, maintainability, ai scalability.
- Most campus networks feature a high-performance, switched backbone, called the campus backbone.
- A high-capacity, centralized server farm connects the backbone and provides internal server resources to users, for example, application, file, print, e-ma and Domain Name System (DNS) services.
- Network management is an important component in a camp network design.
- A campus backbone must provide access to management devices that support monitor logging, troubleshooting, security, and other common management functions.

The campus infrastructure module has three submodules:

- **Building access submodule**: Located within a campus building, this submodule contains end-u workstations and IP phones connected to switches or wireless access points. Higher-end switches provide uplinks to the building distribution module. Services offered by this module include netw access, broadcast control, protocol filtering, and the marking of packets for QoS features.

- **Building distribution submodule**: The job of this submodule is to aggregate wiring closets with a building and provide connectivity to the campus backbone via routers (or switches with routing modules). This submodule provides routing, QoS, and access control methods for meeting secure and performance requirements. Redundancy and load sharing are recommended for this submodule.

- **Campus backbone:** The campus backbone is the core layer of the campus infrastructure. The backbone interconnects the building access and distribution submodules with the server farm, network management, and edge distribution modules. The campus backbone provides redundancy and fast-converging connectivity. It routes and switches traffic as quickly as possible from one module to another. This module usually uses high-speed routers (or switches with routing capabilities and provides QoS and security features.