

# Cisco Enterprise Architecture Model

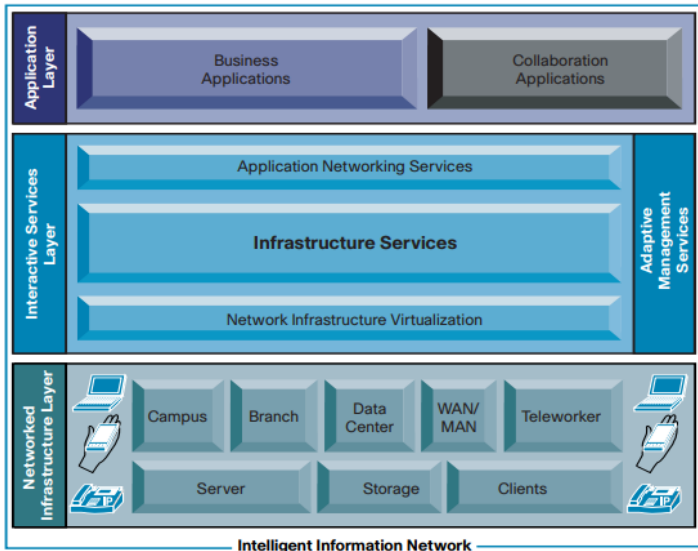
# Cisco Enterprise Architecture Model

- To accommodate the need for modularity in network design, Cisco developed the ***Cisco Enterprise Architecture model***. This model provides all the benefits of the hierarchical network design on the campus infrastructure, and facilitates the design of larger, more scalable networks.
- The Cisco Enterprise Architecture model separates the enterprise network into functional areas that are referred to as modules. The modularity that is built in to the architecture allows flexibility in network design and facilitates implementation and troubleshooting.

## **Cisco service oriented network architecture (SONA)**

- Enabling rapid adoption and deployment of new application services at a reduced cost of development and overhead
- Coordinating application and network events with business process to speed business agility Enforcing business policies in the application and network infrastructure to improve security and reduce risk.
- Aligning network resources to applications to meet business objectives to provide a competitive differentiation.

# Figure: Cisco Service-Oriented Network Architecture



## The benefits of SONA

- **Functionality:** Supports the organizational requirements.
- **Scalability:** Supports growth and expansion of organizational tasks by separating functions and products into layers; this separation makes it easier to grow the network.
- **Availability:** Provides the necessary services, reliably, anywhere, anytime.
- **Performance:** Provides the desired responsiveness, throughput, and utilization on a per application basis through the network infrastructure and services.
- **Manageability:** Provides control, performance monitoring, and fault detection.
- **Efficiency:** Provides the required network services and infrastructure with reasonable operational costs and appropriate capital investment on a migration path to a more intelligent network, through step-by-step network services growth.
- **Security:** Provides for an effective balance between usability and security while protecting information assets and infrastructure from inside and outside threats.

## Three Layers of Cisco SONA

1. **The networked infrastructure layer**, where all the IT resources are interconnected across a converged network foundation.
  - At the networked infrastructure validated Cisco enterprise architectures provide complete design guidance for a fully integrated end-to-end system across your entire network.
  - The IT resources include servers, storage, and clients.
  - The Networked Infrastructure layer represents how these resources exist in different places in the network, including the campus, branch, data center, enterprise edge, WAN, metropolitan-area network (MAN), and with the teleworker.
  - The objective of this layer is to provide connectivity, anywhere and anytime.
  - The Networked Infrastructure layer includes the network devices and links to connect servers, storage, and clients in different places in the network.

# The interactive services layer

1. **The interactive services layer**, which enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure.
  - At the interactive services layer, Cisco integrates a complete suite of services into intelligent systems that optimize the delivery of business and collaboration applications for more predictable and reliable performance, while lowering operational costs.
  - This layer enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure.
  - This layer includes the following services:
    - Voice and collaboration services
    - Mobility services
    - Wireless services
    - Security and identity services
    - Storage services
    - Compute services
    - Application networking services (content networking services)
    - Network infrastructure virtualization
    - Adaptive network management services
    - Quality of service (QoS)
    - High availability
    - IP multicast

# The applications layer

1. **The applications layer**, which contains the business applications and collaborative applications that take advantage of efficiencies from the interactive services.
  - At the application layer, by deeply integrating with the network fabric, Cisco application networking solutions require no client installation or application changes while maintaining application visibility and security throughout application delivery.
  - The objective of this layer is to meet business requirements and achieve efficiencies by leveraging the interactive services layer. This layer includes the following collaborative applications:
    - Instant messaging
    - Cisco Unified Contact Center
    - Cisco Unity (unified messaging)
    - Cisco IP Communicator and Cisco Unified IP Phones
    - Cisco Unified MeetingPlace
    - Video delivery using Cisco Digital Media System
    - IP telephony.



primary Cisco Enterprise Architecture modules:

- Enterprise campus
- Enterprise edge
- Service provider edge

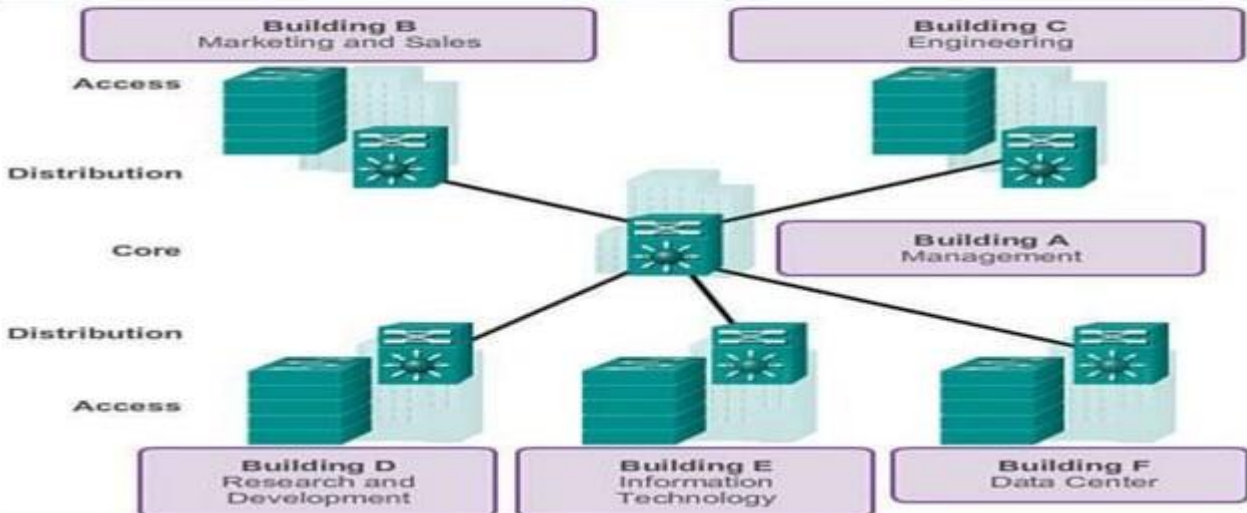
Connected to the service provider edge are the remote modules, including:

- Enterprise branch
- Enterprise teleworker
- Enterprise data center

# Design Principal

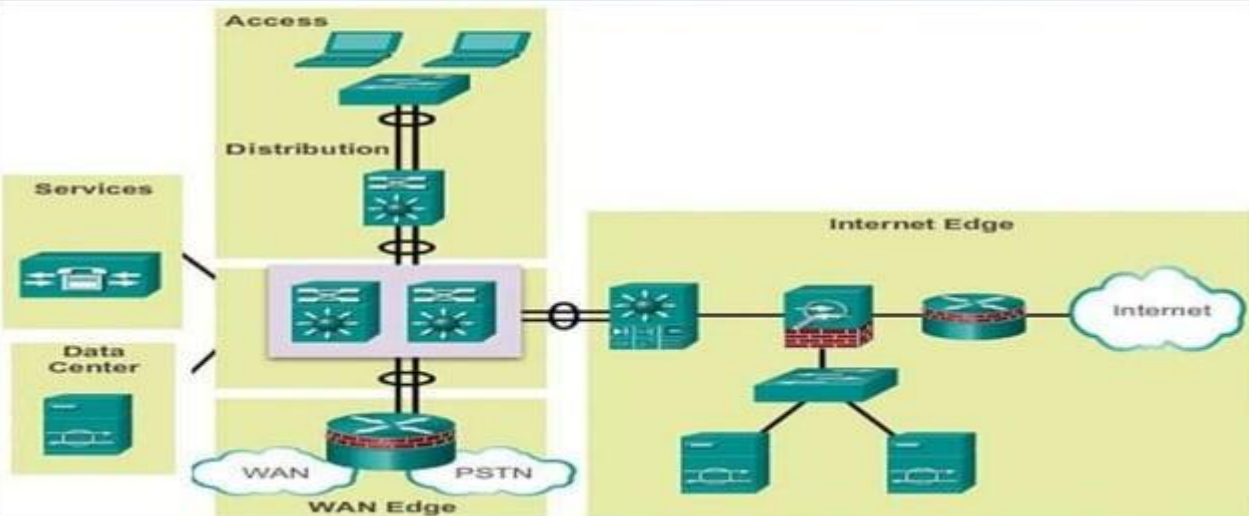
- Hierarchy\*
- Modularity\*
- Resiliency
- Flexibility

# Over View

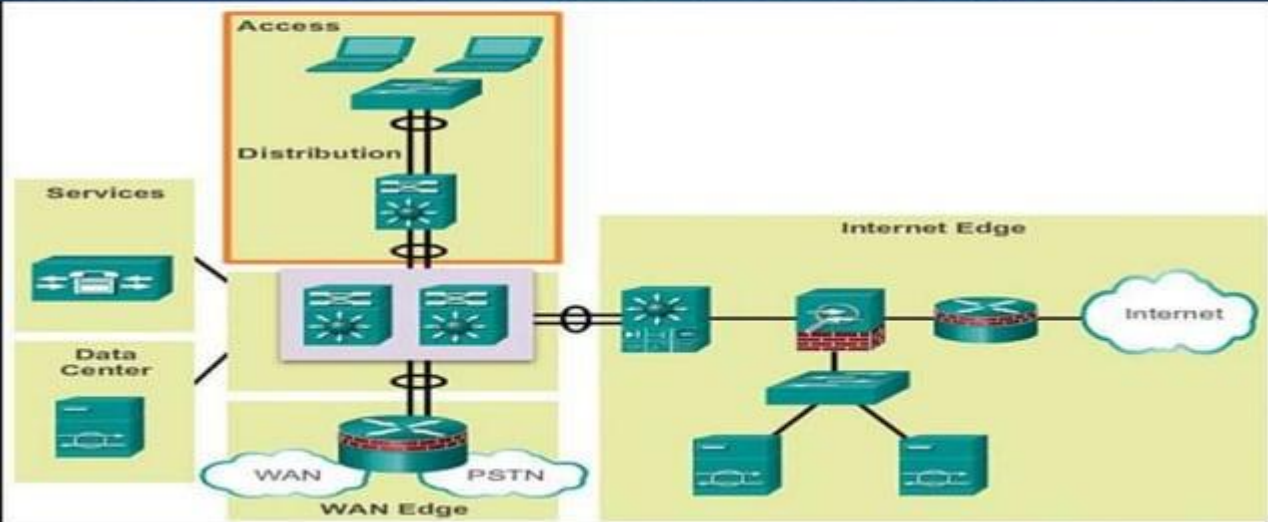


# Modularity

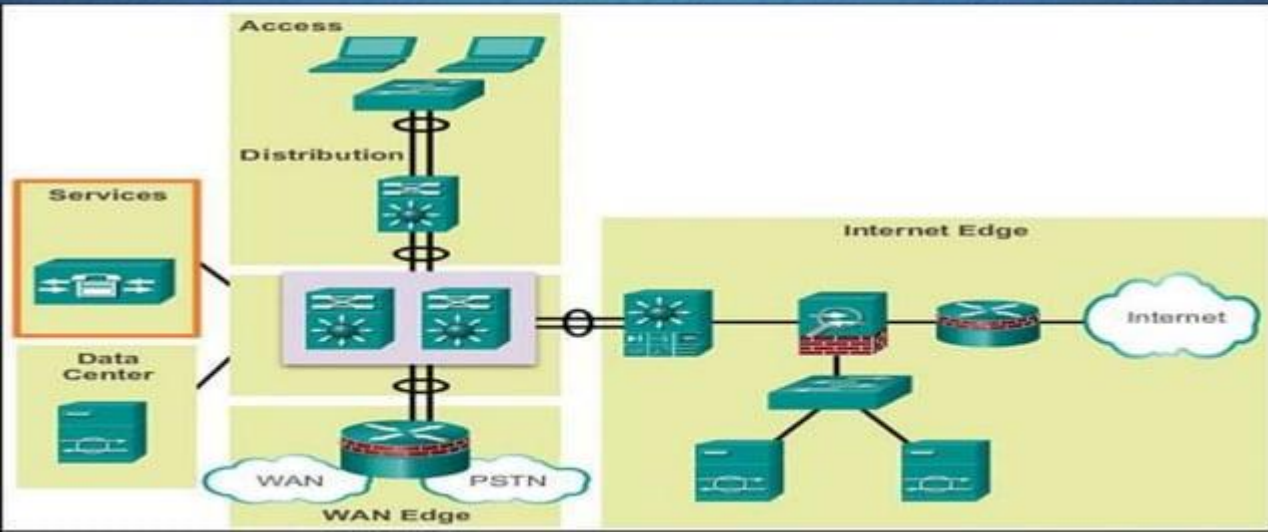
# Over View



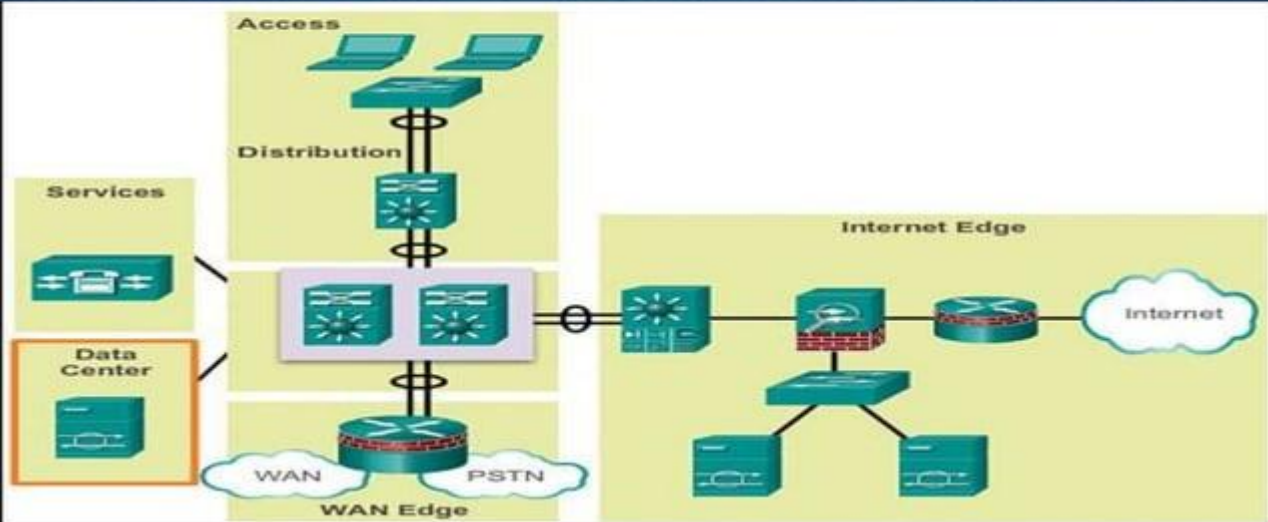
# Access-Distribution Module



# Services Module

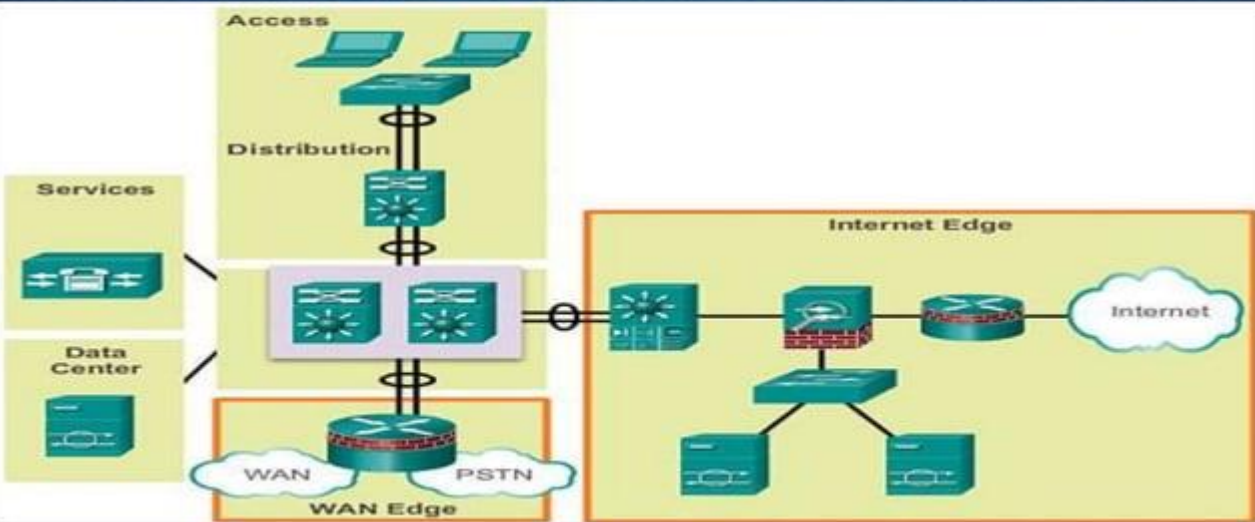


# Data Center Module





# Enterprise Edge Module

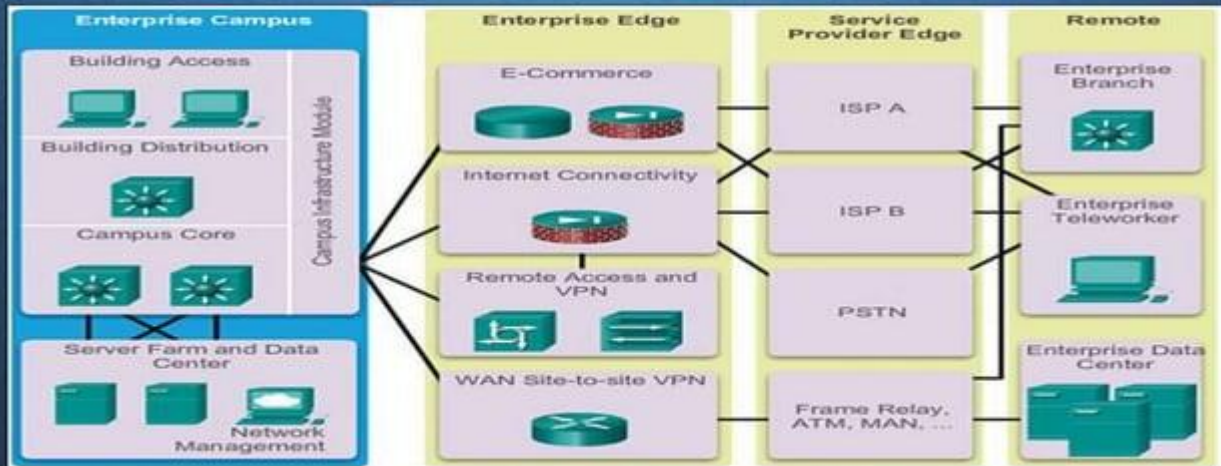


# Modules

- Cisco Enterprise Campus
- Cisco Enterprise Edge
- Service Provider Edge

# Cisco Enterprise Campus Model

# Cisco Enterprise Campus



- A campus network is a building or group of buildings connected into one enterprise network that consists of many LANs. A campus is generally limited to a fixed geographic area, but it can span several neighboring buildings (for example, an industrial complex or business park environment).
- The *enterprise campus module* describes the recommended methods to create a scalable network while addressing the needs of campus-style business operations. The architecture is modular and can easily expand to include additional campus buildings or floors as the enterprise grows.

The enterprise campus module consists of the following submodules:

- Building access
- Building distribution
- Campus core
- Data center

Together these submodules:

- Provide high availability through a resilient hierarchical network design
- Integrate IP communications, mobility, and advanced security
- Utilize multicast traffic and QoS to optimize network traffic
- Provide increased security and flexibility using access management, VLANs, and IPsec VPNs

## Sub Modules

- E-commerce services
- Internet connectivity
- Remote access and VPN access
- WAN site-to-site VPN access

- **E-commerce networks and servers:** The e-commerce submodule enables enterprises to support e-commerce applications through the Internet. It uses the high-availability designs of the data center module. Devices located in the e-commerce submodule include web, application, and database servers; firewall and firewall routers; and network intrusion prevention systems (IPS).
- **Internet connectivity and demilitarized zone (DMZ):** The Internet submodule of the enterprise edge provides internal users with secure connectivity to Internet services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISPs) is also provided. Components of this submodule include firewall and firewall routers, Internet edge routers, FTP and HTTP servers, SMTP relay servers, and DNS servers.
- **Remote access and VPN:** The VPN/remote access submodule of the enterprise edge provides remote-access termination services, including authentication for remote users and sites. Components of this submodule include firewalls, dial-in access concentrators, Cisco Adaptive Security Appliances (ASA), and network intrusion prevention system (IPS) appliances.
- **WAN:** The WAN submodule uses various WAN technologies for routing traffic between remote sites and the central site. Enterprise WAN links include technologies such as Multiprotocol Label Switching (MPLS), Metro Ethernet, leased lines, Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), PPP, Frame Relay, ATM, cable, digital subscriber line (DSL), and wireless.

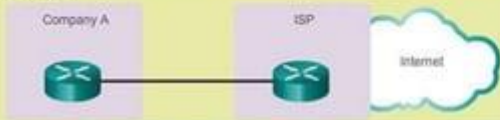


## **The SP edge module**

- Spans across large geographic areas in a cost effective manner
- Converges voice, video, and data services over a single IP communications network
- Supports QoS and service level agreements
- Supports security using VPNs (IPsec / MPLS) over Layer 2 and Layer 3 WANs

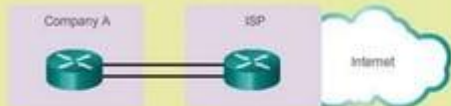
# Cisco Service Provider Edge Types

Single-homed

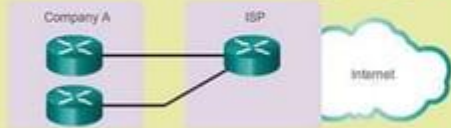


Dual-homed

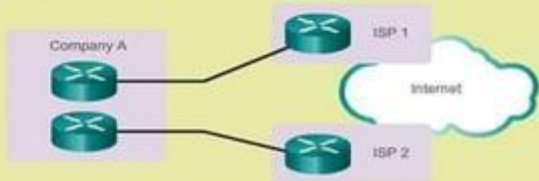
Option 1



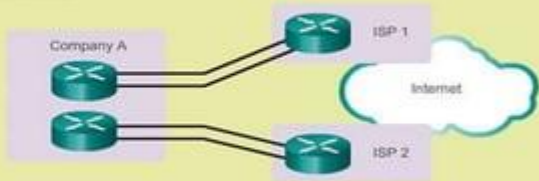
Option 2



Multihomed



Dual-multihomed



- When acquiring Internet services from an ISP, redundancy or failover should be considered. Redundant Internet connections vary depending if the enterprise is connecting to a single ISP or multiple ISPs.

As shown in [Fig](#), redundant connections to a single ISP can include

- **Single-homed:** A single connection to an ISP
- **Dual-homed:** Two or more connections to a single ISP

## Sub Modules

- Enterprise Branch
- Enterprise Teleworker
- Enterprise Data Center

# Enterprise Branch

- The *enterprise branch module* includes remote branches that allow employees to work at non campus locations.
- These locations are typically responsible for providing security, telephony, and mobility options to employees, as well as general connectivity into the campus network and the different components located inside the enterprise campus.
- The enterprise branch module allows enterprises to extend head-office applications and services, such as security, Cisco Unified Communications, and advanced application performance, to the remote branches.
- The edge device connecting the remote site to the central site varies depending on the needs and size of the site. Large remote sites may use high-end Cisco Catalyst switches, while smaller sites may use an ISR G2 router.
- The enterprise branch module connects to the enterprise campus site primarily using a WAN link. However, it also has an Internet link as a backup. The Internet link uses site-to-site IPsec VPN technology to encrypt corporate data.

# Enterprise Teleworker

- The *enterprise teleworker module* is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites.
- The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL.
- VPN services can then be used to secure communications between the mobile worker and central campus. Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker.
- Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

# Enterprise Data Center

- The *enterprise data center module* is a data center with all of the same functional options as a campus data center, but exists at a remote location.
- This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise.
- High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center.
- Redundant data centers provide backup using synchronous and asynchronous data and application replication.
- Additionally, the network and devices offer server and application load balancing to maximize performance.