CSET 150

NETWORK DESIGN AND MANAGEMENT

EVENING MASTERS EDITION

DR. MAHBOOB QAOSAR

ASSOCIATE PROFESSOR, CSE, RU

COURSE CONTENTS

Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations, IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

Mitigating Technologies

- Mitigating Technologies
  - ~~Threat Defense~~
  - ~~Secure communication~~
  - ~~Trust and identity~~
  - Network security best practices

Network security best practices

- 3 issues:
  1. **Network Management**
  2. **Assessment and Audits**
  3. **Policies**

Network Management

- There is a saying in network security: "**If you log it, read it."**
- … firewalls, routers, and IDSs, can send **syslog** security triggers to a central repository such as a **syslog** server
- Nonsense … if not use the log
- … **security event management software** should be used
- If a significant anomaly be discovered…
- In addition, correlation tool modules can be added to assist the network administrator …

Assessment and Audits

- Prior to designing your network, you should conduct a **security assessment** to uncover **potential vulnerabilities** and therefore target your security efforts where they are the most effective.

- Subsequently, when your network security systems are in full production, it can be beneficial **to hire a security audit company** that can perform penetration testing and report on the corporate network security position.

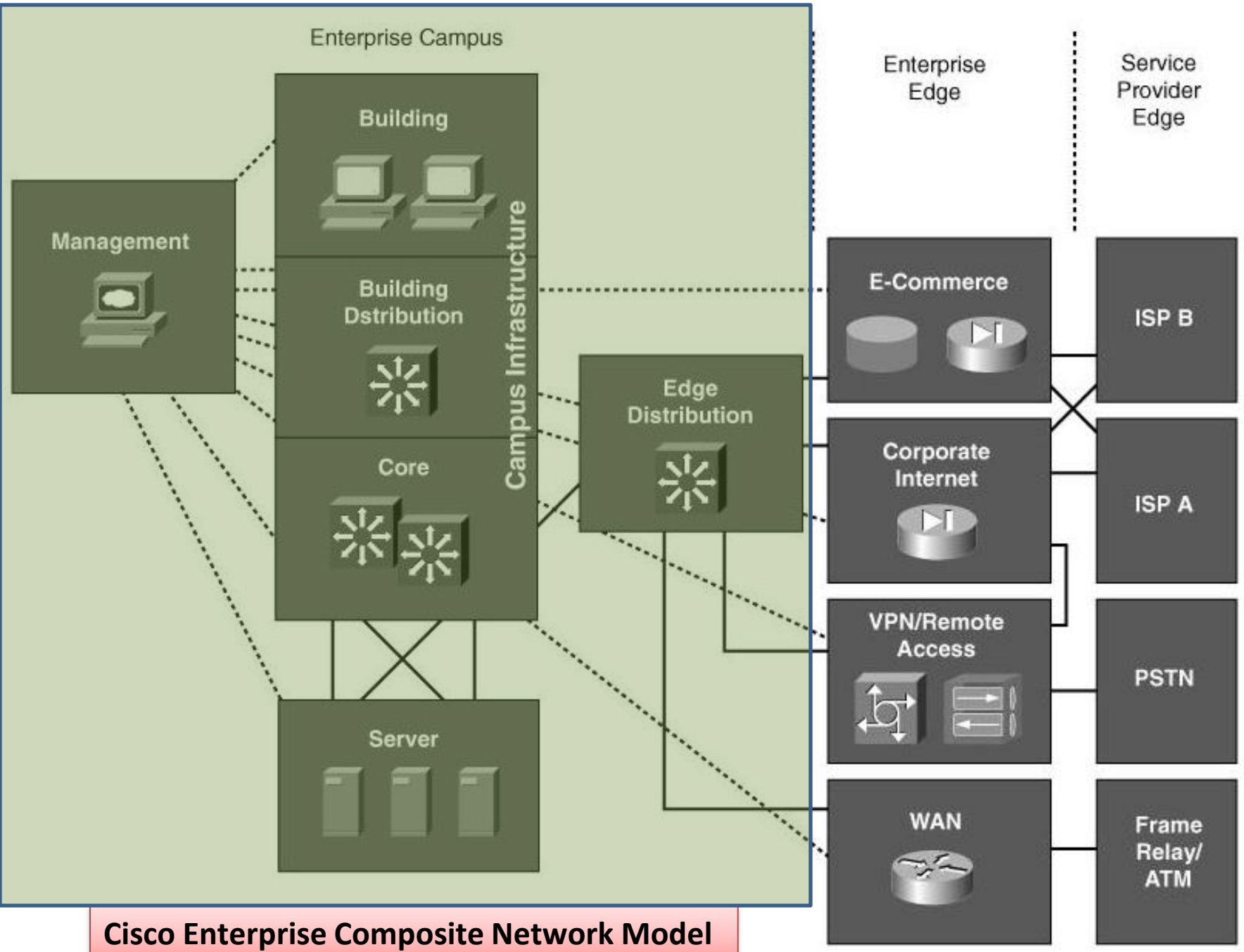
POLICES

- Organizations must develop basic network policies, disseminate them, and enforce them:
  1. Internet usage policy
  2. E-mail usage policy
  3. Remote-access policy
  4. Password-handling policy
  5. Software and hardware installation policy
  6. Physical security policy
  7. Business continuity policy

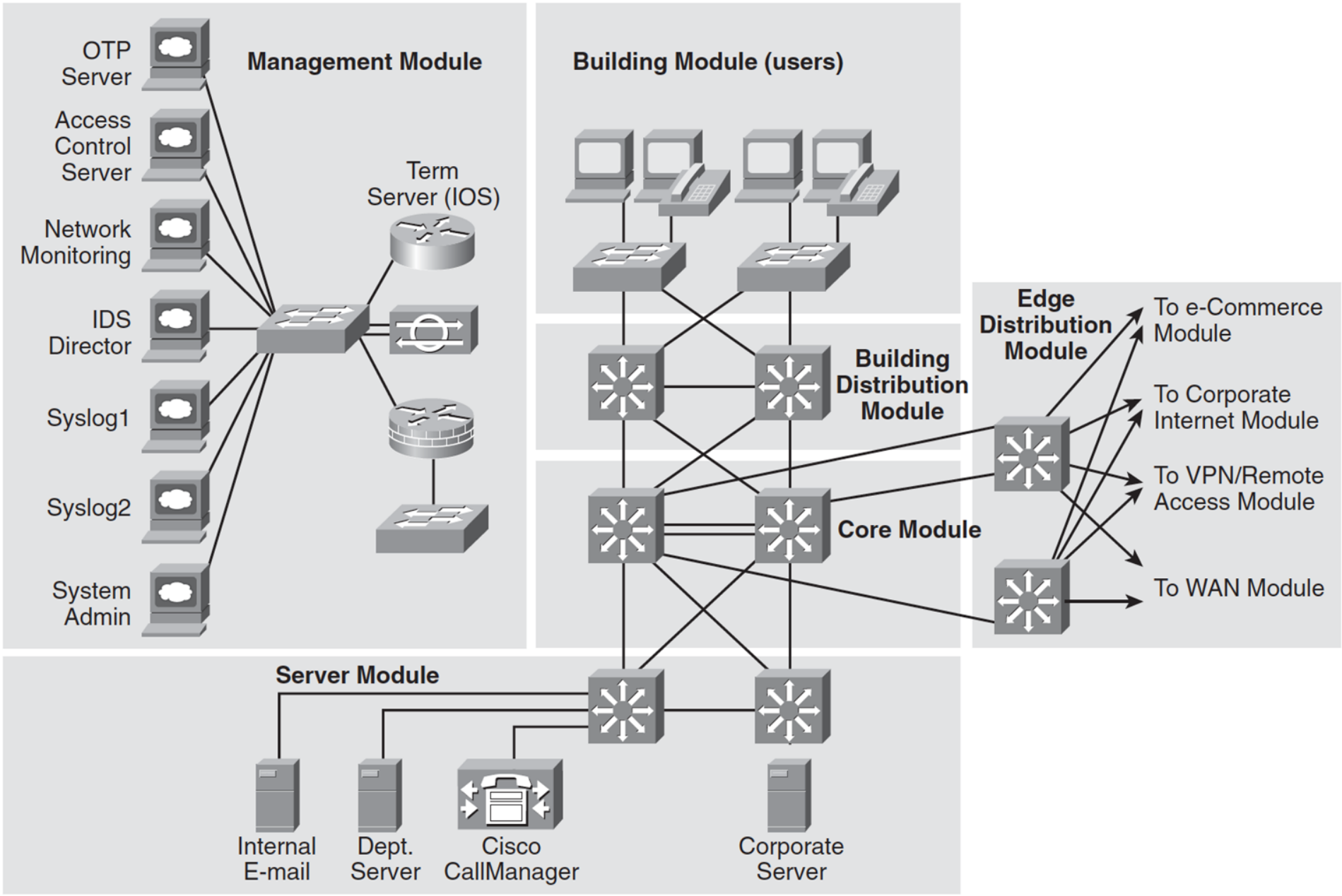
SAFE CAMPUS DESIGN

- Cisco has developed a guide, called the **Cisco SAFE Blueprint**,
- **Cisco SAFE Blueprint - - -** -of best practices for designing and securing networks
- **Cisco Enterprise Composite Network Model** --- is the name given to the architecture used by the SAFE blueprint.
- At the highest layer, this model divides an enterprise network into the following **three main functional areas:**

1. ENTERPRISE CAMPUS
2. ENTERPRISE EDGE
3. SERVICE PROVIDER EDGE



Cisco Enterprise Composite Network Model

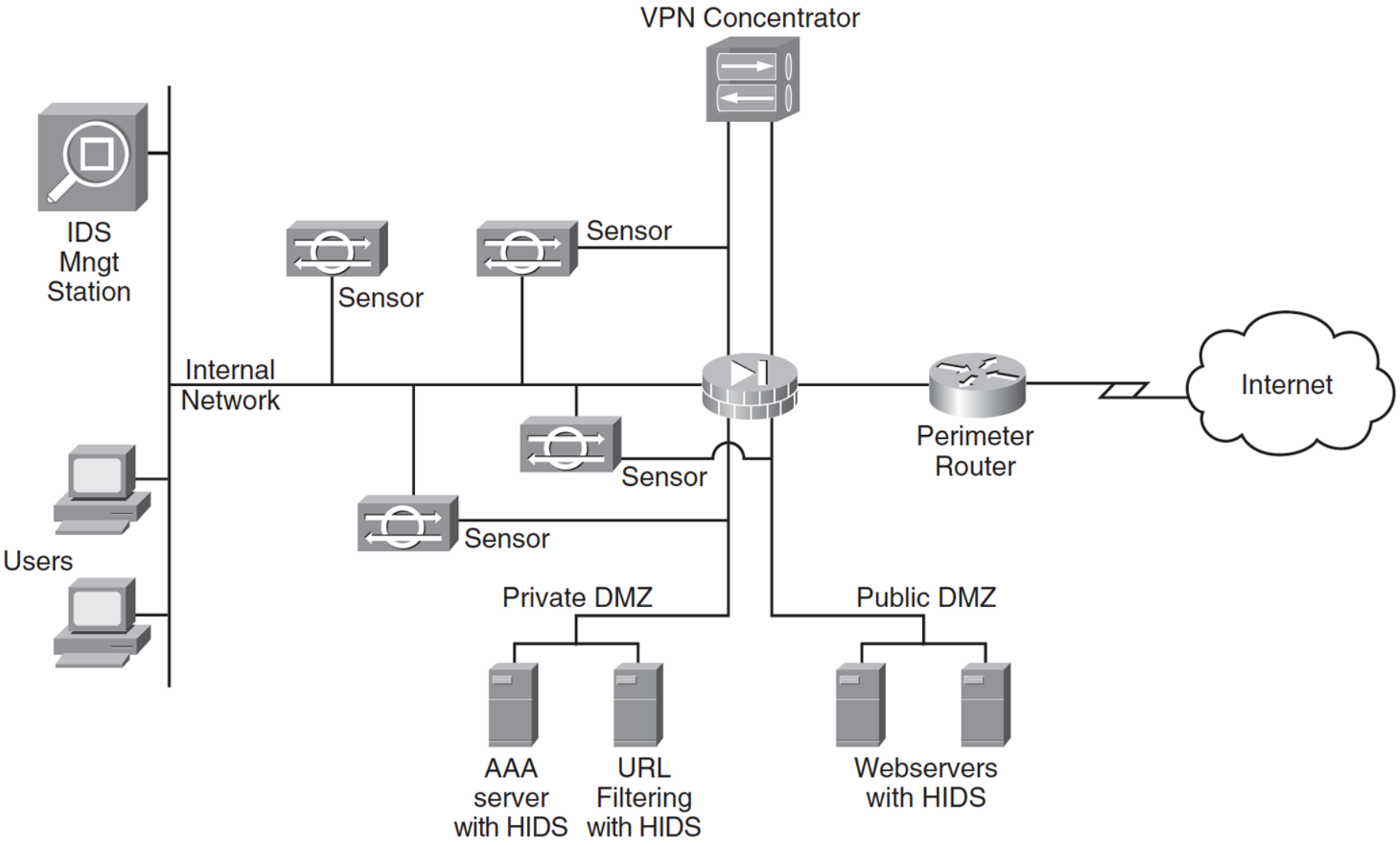

OTP Server
Access Control Server
Network Monitoring
IDS Director
Syslog1
Syslog2
System Admin
Management Module
Term Server (IOS)
Building Module (users)
Building Distribution Module
Core Module
Edge Distribution Module
To e-Commerce Module
To Corporate Internet Module
To VPN/Remote Access Module
To WAN Module
Server Module
Internal E-mail
Dept. Server
Cisco CallManager
Corporate Server

Out-of-band (OOB) management is a method of remotely controlling and managing critical IT assets and network equipment using a secure connection through a secondary interface that is physically separate from the primary network connection. This enables administrators to gain control even during infrastructure faults.

Enterprise Campus Module	Key Devices	Special Security Design Considerations
Network Management Module	HIDS Virus scanning OTP server Access Control Server Network log server Layer 2 switch	Out-of-band management should be preferred over in-band management. If in-band management must be used, employ IPsec, SSL, or SSH.

Enterprise Campus Module	Key Devices	Special Security Design Considerations
Core Module	Layer 3 switch	No special consideration, other than the fact that switches are a target and should be protected. We explain this in Chapter 2, "Switching Design."
Building Distribution Module	Layer 3 switch	VLANs can be used to further segment the different departments within a campus.
Building Module (corporate user access)	Layer 2 switch Host virus scanning Network Admission Control	A switched environment is recommended to reduce the risk of packet sniffing.
Server Module	Layer 3 switch HIDS	Often the target of internal attacks, servers should not only be physically secured and running an IDS but should also be kept up to date with the latest patches.

Enterprise Campus Module	Key Devices	Special Security Design Considerations
Edge Distribution Module	Layer 3 switch	Depending on the size of the infrastructure, the Edge Distribution Module can be folded into the Core Module. In this case, an IDS should be included in the Core Module. This could be done with the insertion of an IDS card in the Layer 3 switch.


VPN Concentrator
IDS
Mngt
Station
Sensor
Sensor
Sensor
Internal
Network
Sensor
Sensor
Perimeter
Router
Internet
Users
Private DMZ
Public DMZ
AAA
server
with HIDS
URL
Filtering
with HIDS
Webservers
with HIDS

COURSE CONTENTS

Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations, IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

Chapter 5

WIRELESS LAN DESIGN

WLAN

- The popularity of WLANs is undeniable.

- The following **03 main** driving forces play in favor of WLANs:
  1. FLEXIBILITY
  2. INCREASED PRODUCTIVITY
  3. COST SAVINGS COMPARED TO WIRED DEPLOYMENT

FLEXIBILITY

- WLANs let users access servers, printers, and other network resources regardless of their location, within the wireless reach.
- This flexibility means that, for example, a user's laptop stays connected working from a colleague's cubicle, from a small meeting room, or from the cafeteria.
- Recognizing the benefits brought about by WLAN flexibility, businesses are now deploying WLANs in record numbers.

INCREASED PRODUCTIVITY

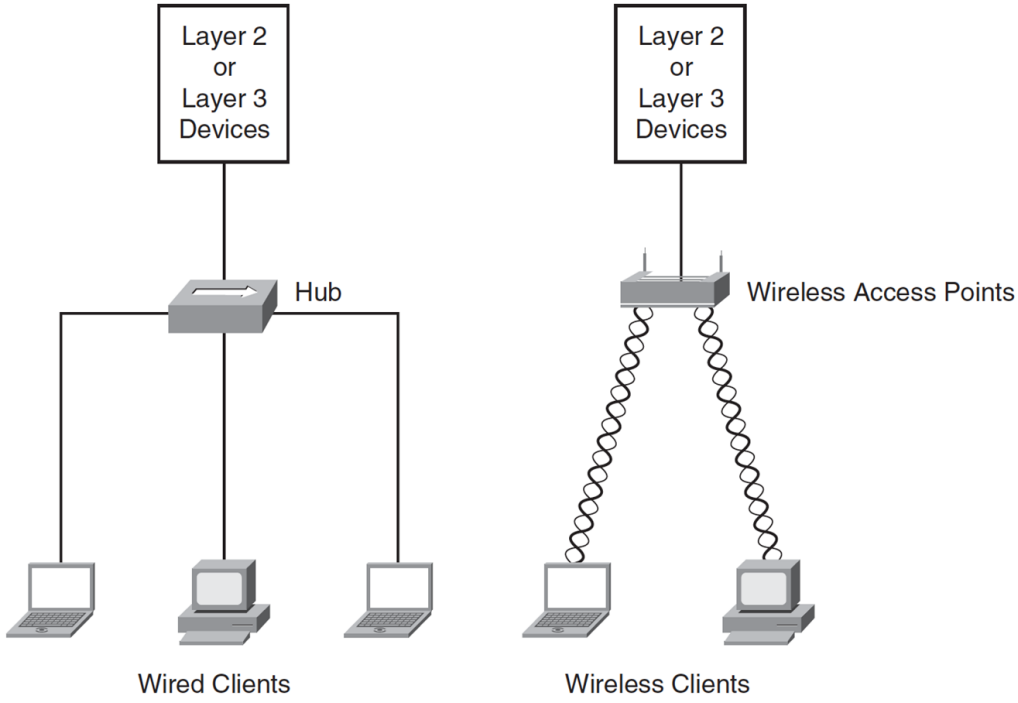
- According to a 2003 NOP World research study, WLAN users stayed connected to their corporate network **3.64 hours per day longer** than their wired peers, thus increasing their productivity **by 27 percent**.
- Through the flexibility of WLANs, not only does the productivity go up, **but the response times** are also significantly improved

COST SAVINGS

- Another --- WLANs is their **low-cost deployment** in locations where the costs of running LAN wire would be prohibitive.
- The total cost of ownership (TCO) of a WLAN is very low compared to the benefits they bring to an organization, providing that a WLAN is secured and managed properly.
- Companies that are not deploying WLANs quickly enough find that employees take the matter in their own hands and install their own WLANs, potentially **creating significant breaches** in the corporate network security infrastructure

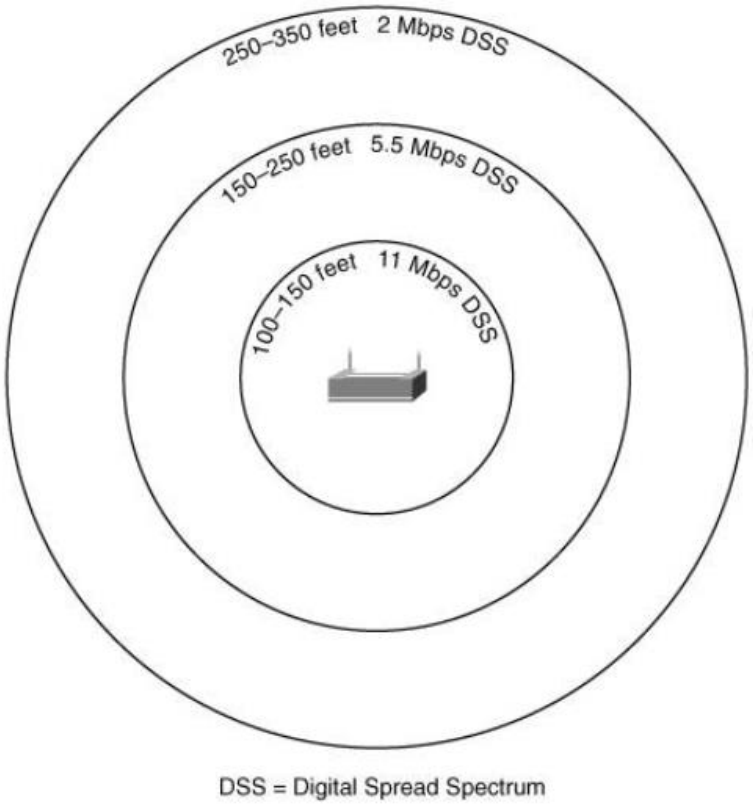
WIRELESS TECHNOLOGY OVERVIEW

- a WLAN is an LAN that uses radio frequency (RF) to communicate instead of using a wire
- Wireless clients connect to wireless access points (WAPs).



WIRELESS TECHNOLOGY OVERVIEW

- Because WLANs use RF, the throughput (speed) is inversely proportional to the distance between the transmitter and the receiver.
- Therefore, everything being equal (notwithstanding interferences), the closer a wireless client is to a transmitter, the greater is the throughput
- Wireless communication brings a **trade-off** between:
  - flexibility and mobility versus battery life and usable bandwidth.

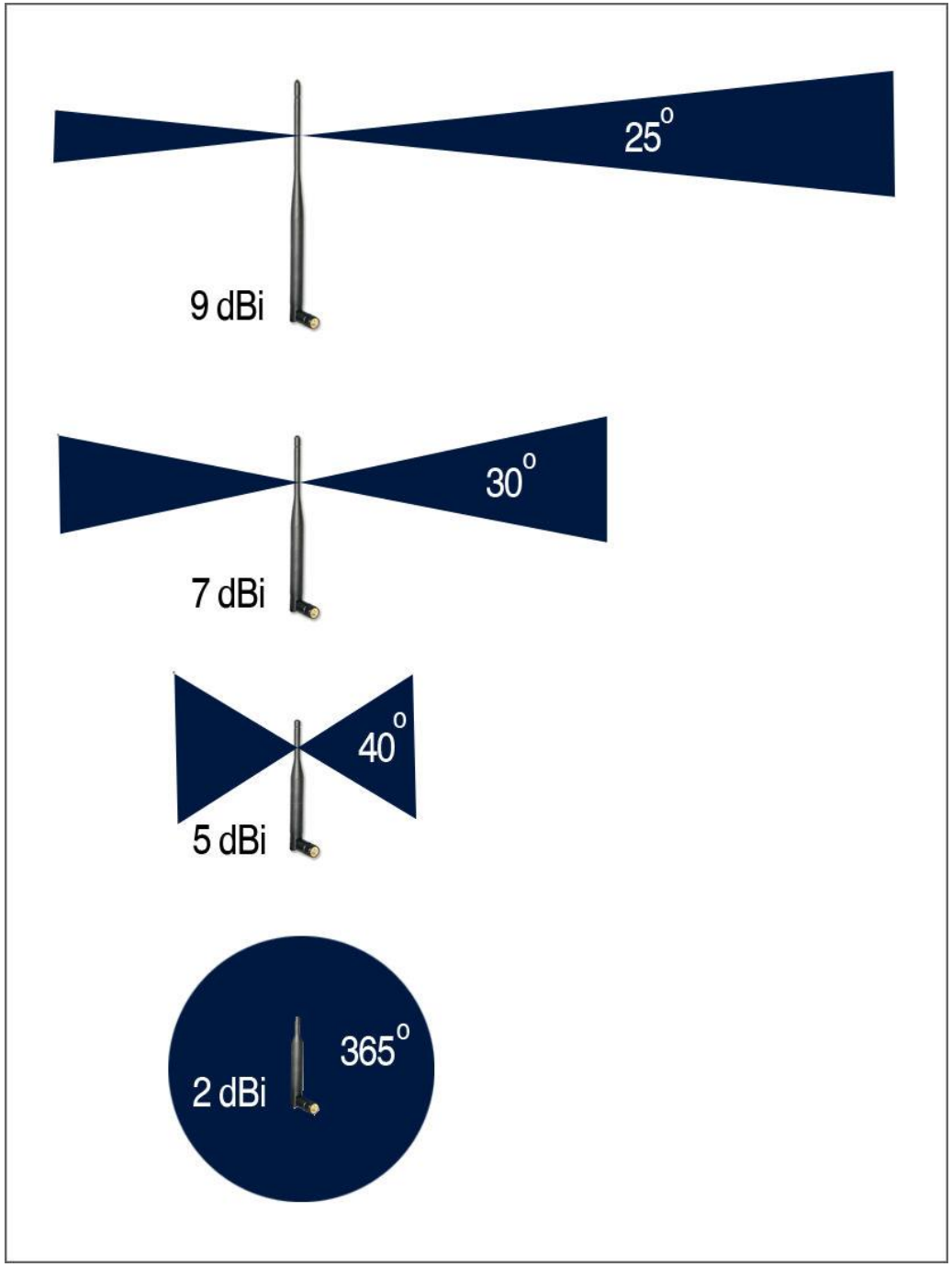


WIRELESS STANDARDS

Table 5-1. Wireless Standards

Standard	Maximum Throughput (Mbps)	Frequency (GHz)	Compatibility	Ratified
802.11b	11	2.4		1999
802.11a	54	5		1999; Product availability 2001
802.11g	54	2.4	Backward-compatible with 802.11b	2003

802.11 Protocol	Freq (GHz)	Bandwidth (MHz)	Approximate indoor range	Approximate outdoor range	
-	2.4	20	20 m / 66 ft	100 m / 330 ft	2Mbps
a	3.7 - 5	20	35 m / 115 ft	120 m / 390 ft	54 Mbps
b	2.4	20	35 m / 115 ft	140 m / 460 ft	11Mbps
g	2.4	20	38 m / 125 ft	140 m / 460 ft	54 Mbps
n	2.4 - 5	20 - 40	70 m / 230 ft	250 m / 820 ft	100 Mbps


25°
9 dBi
30°
7 dBi
40°
5 dBi
365°
2 dBi