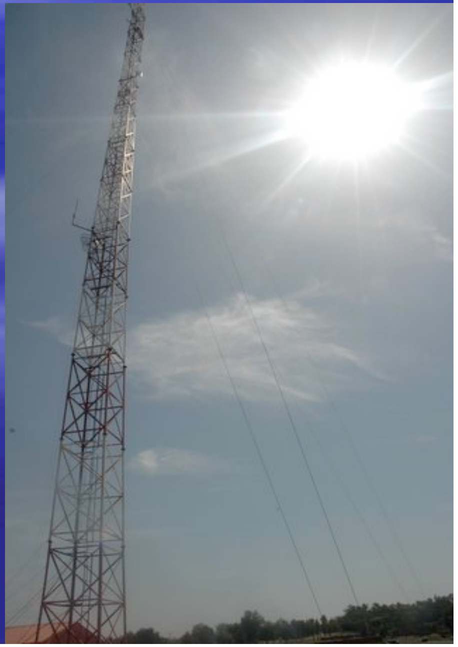
PART B:

Designing, Developing and Implementing a University Network: Wired and Wireless Infrastructure in a Rural Environment"



OUTLINE

- Introduction
  - Evolution of Wired & Wireless Networks
  - Wired & Wireless LAN in the Enterprise

- LAN Design Paradigm

- Wired Local Area Networks

OUTLINE –Cont'd

- Design Considerations in Wireless Local Area Networks
  - Speed/Standards
  - Coverage (How far the signal reaches)
  - Density (How many clients can connect concurrently)

OUTLINE – Cont'd

- Security Issues

  - Standards (802.11, 802.1x etc)
  - Authentication/Access
  - Authorization
  - Encryption

- RF planning/Management

OUTLINE – Cont'd

- Design, Developing and Implementing Wired/Wireless Networks – AAUN Case Study
- Summary

EVOLUTION

- Mooted in the late 1960s

- About 10 years ago, different standards, Topology and Access Media were Prevalent (Token Ring, ARCNET, Thick net, Thin net etc)

- Media such as Coaxial Cables, Shielded Twisted Pair etc were predominantly in Use for LAN Deployment

EVOLUTION

- Today, the Ethernet standard is predominant with UTP and Fiber as choice Media

- Wireless standard was ratified by the IEEE in 1997 under the 802.11 Ethernet standard

- The 802.11 Wireless had up to 2Mbps speed

WIRED & WIRELESS LAN IN THE ENTERPRISE

- The Enterprise Networks today runs basically on Ethernet and other Variants

- Structured Wired & Wireless LANs are Easier to Deploy and Manage than Ad-Hoc solutions

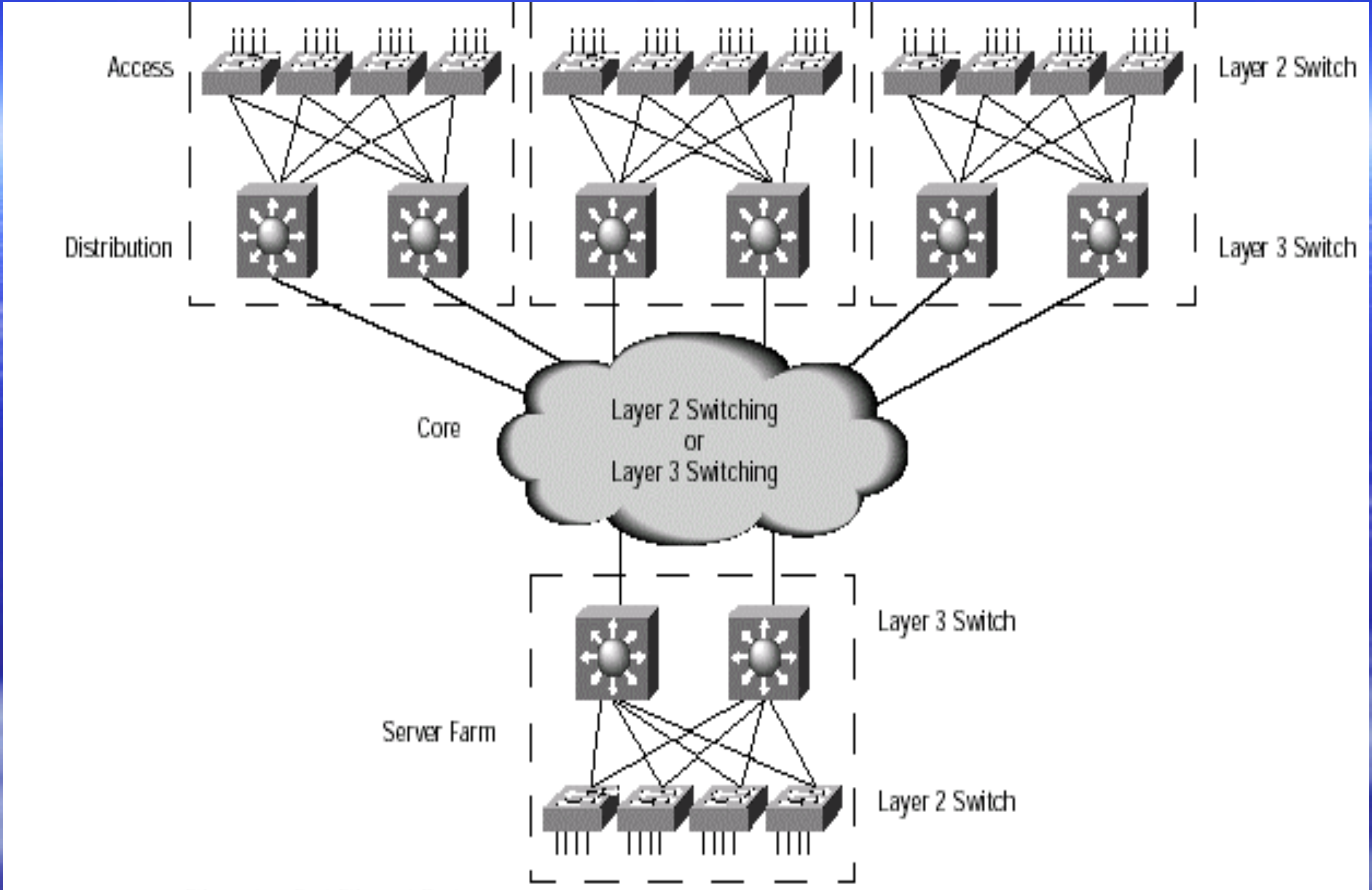
- Standards Have been developed over time in the deployment of Wired & Wireless LANs

LAN DESIGN PARADIGM

LAN Architecture are either:

- **FLAT or HIERACHICAL**
  (Wired Local Area Networks)

- **DISTRIBUTED or CENTRALIZED**
  (Wireless Local Area Networks)



Hierarchical Network Design

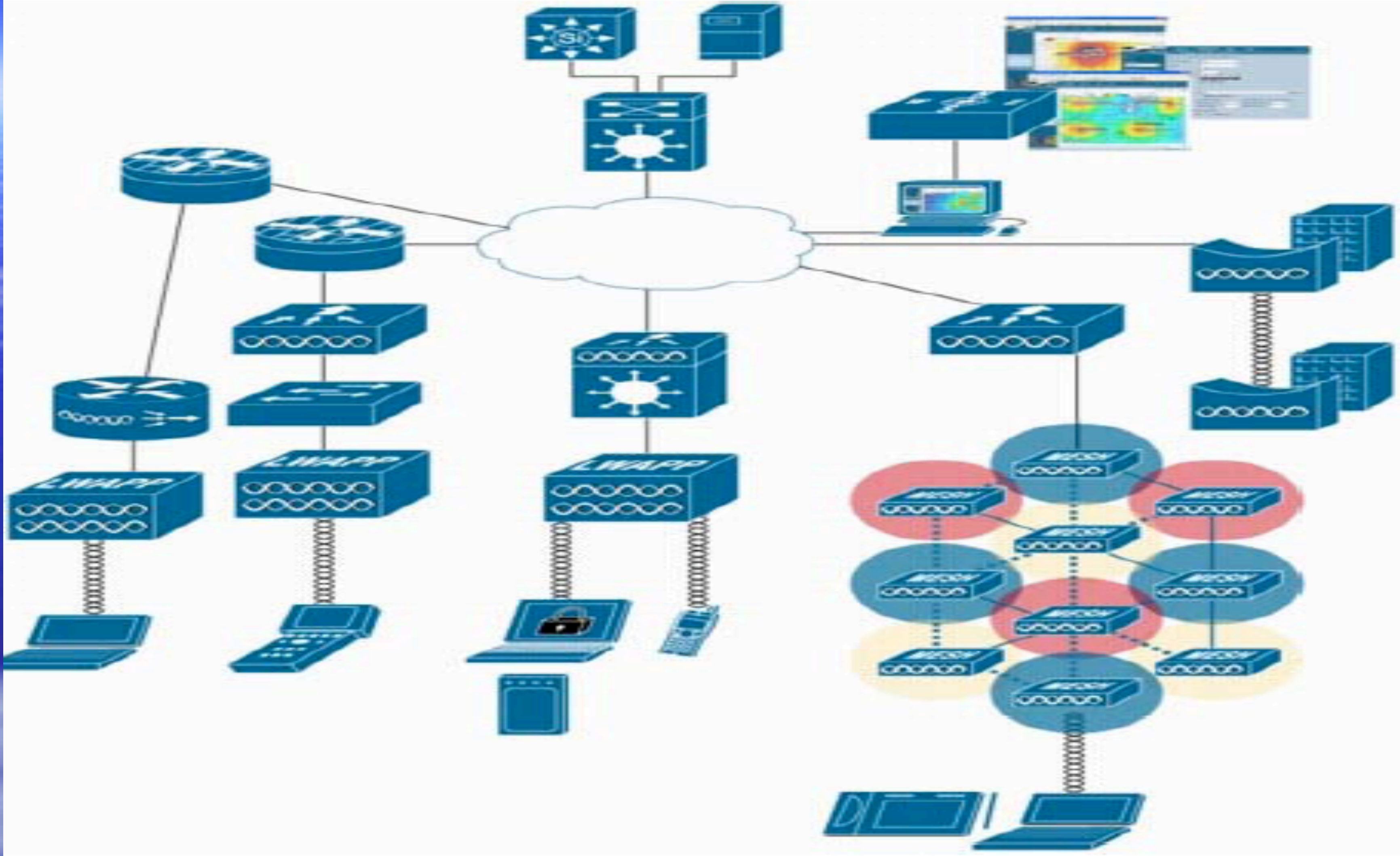
WIRED LANs

- Structured Wired LAN consists of the following components:
  - Cabling Infrastructure (Cables, Trunks or Casing, Patch Panels, Patch cables, Data Outlets, cabinets etc)
  - Active Equipments (Switches, Hubs, Routers etc)
  - End Devices and Interfaces (Servers, Workstations, NICs etc)
  - Appropriate Labels

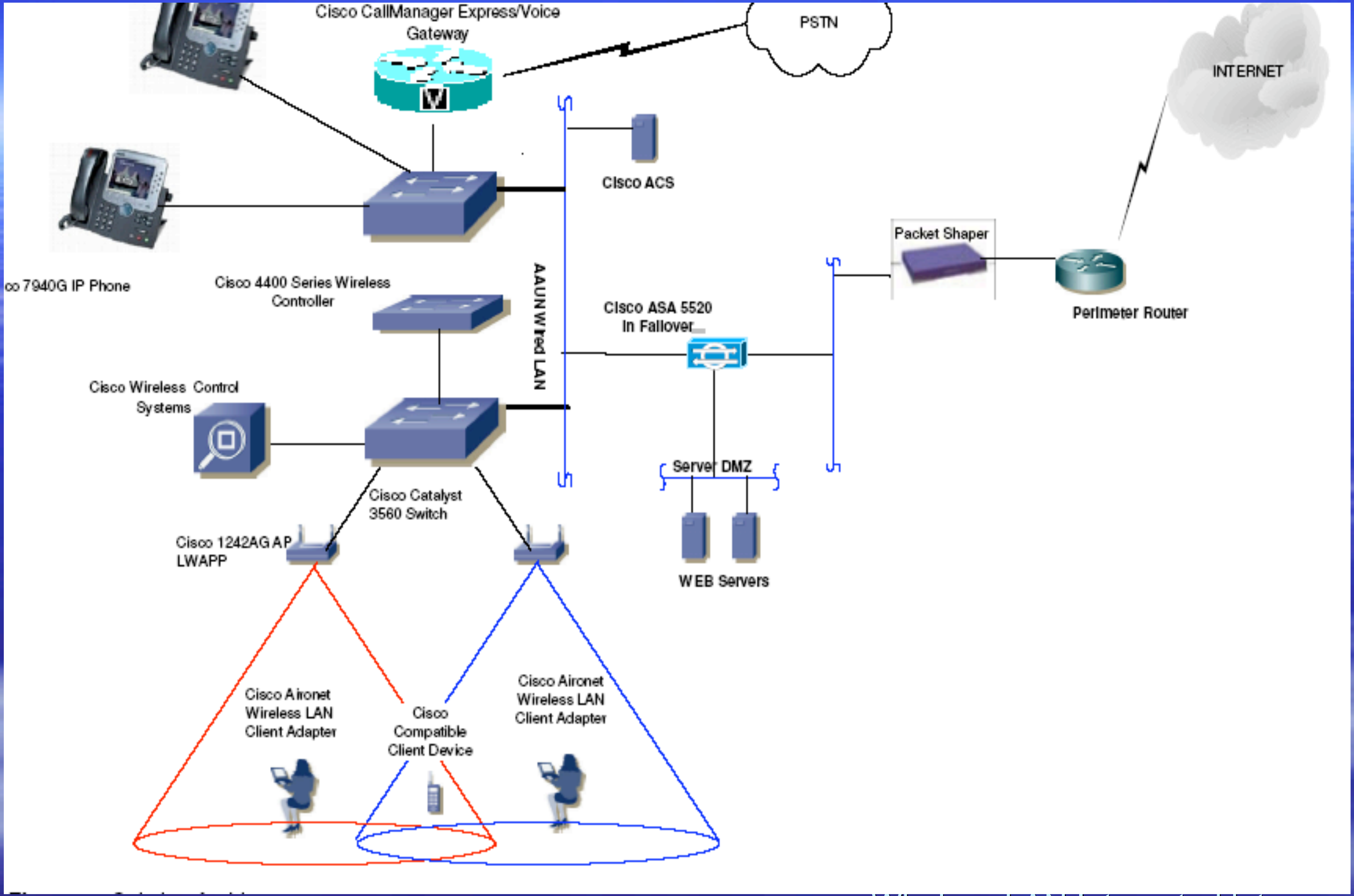
WIRELESS LANs

- Wireless LANs like wired LAN consists of the following components:
  - Access Points or Base stations & Antenna)
  - Active Equipment (Switches, Hubs, PoE etc)
  - Backbone (Connection to the Wired LAN)
  - Wireless LAN Controller & Control System (Optional)
  - RF Planning tool (Optional)
  - Security Components

Access Point

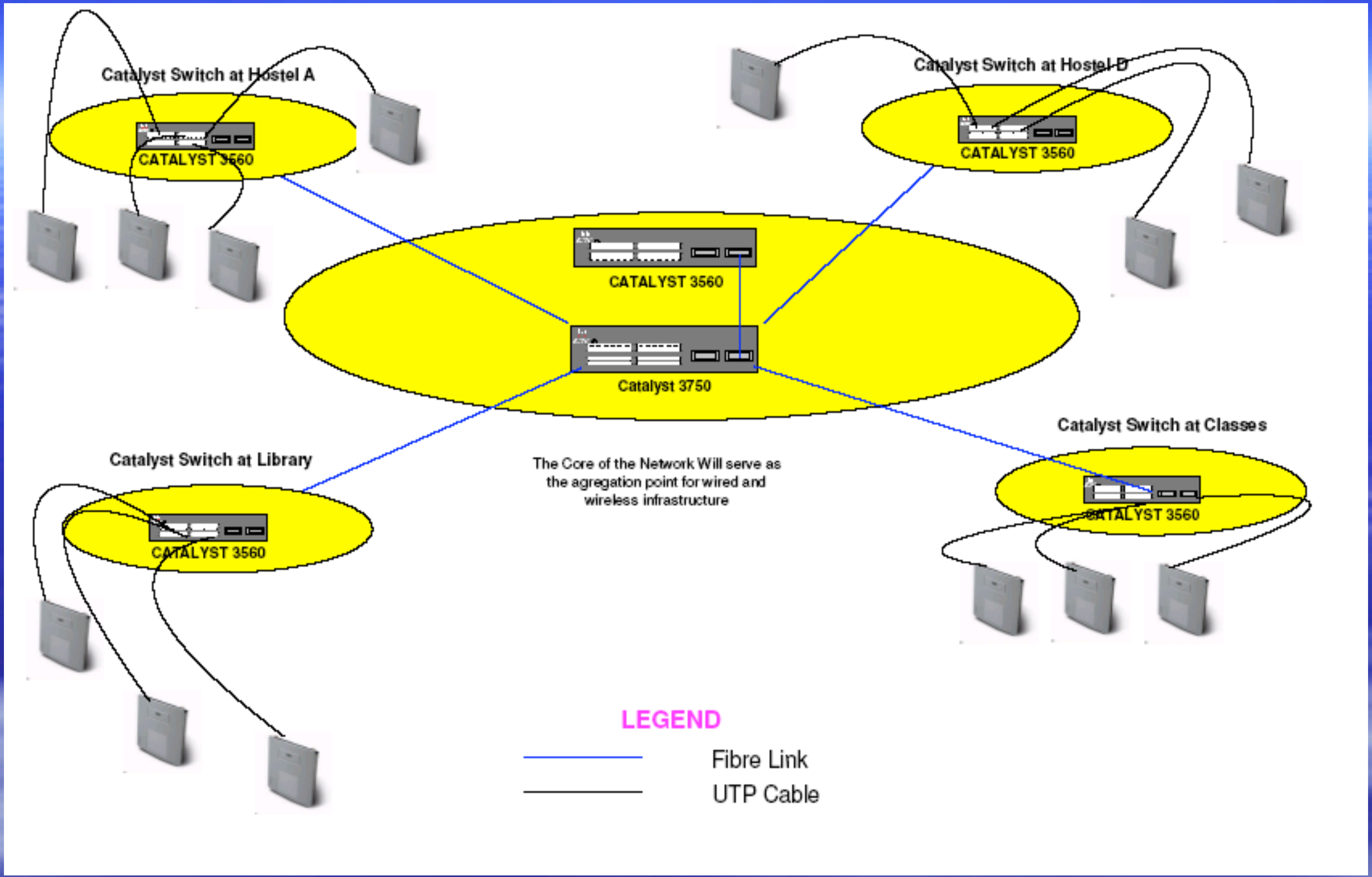


Wireless LAN Architecture & Components


Cisco CallManager Express/Voice Gateway
PSTN
INTERNET
Cisco ACS
co 7940G IP Phone
Cisco 4400 Series Wireless Controller
AAUN Wired LAN
Cisco ASA 5520 In Failover
Packet Shaper
Perimeter Router
Cisco Wireless Control Systems
Server DMZ
Cisco Catalyst 3560 Switch
Cisco 1242AG AP LWAPP
WEB Servers
Cisco Aironet Wireless LAN Client Adapter
Cisco Compatible Client Device
Cisco Aironet Wireless LAN Client Adapter

Wireless LAN Integrated into Wired LAN

Wireless LAN Backbone


Catalyst Switch at Hostel A
CATALYST 3560
Catalyst Switch at Hostel D
CATALYST 3560
CATALYST 3560
Catalyst 3750
Catalyst Switch at Classes
CATALYST 3560
Catalyst Switch at Library
CATALYST 3560
LEGEND
Fibre Link
UTP Cable

The Core of the Network Will serve as the agregation point for wired and wireless infrastructure

DESIGN CONSIDERATION IN WLAN

- There are special consideration in the design of WLAN. These are:
- Speed/Standards : 802.11,a,b or g
- Coverage
- Density
- Security
- Power
- RF Planning/Management

DESIGN CONSIDERATION IN WLAN-SPEED/STANDARD

- 802.11 standard ratified in 1997 had :
- Data rate up to 2Mbps in the 2.4GHz frequency space (Industry Scientific Medical) –ISM Frequency
- Used Frequency-Hopping Spread Spectrum (FHSS) or Direct Sequencing Spread Spectrum (DSSS) modulation
- WEP & WPA Security Mechanism

DESIGN CONSIDERATION IN WLAN-SPEED/STANDARD

- 802.11 standard ratified in 1997 had was extended to 802.11b in July 1999 :
- With theoretical data rate up to 11Mbps in the 2.4GHz band (ISM Band)
- Uses Direct Sequencing Spread Spectrum (DSSS) modulation with 3 non-overlapping channels
- Interference from other appliances in the 2.4GHz Band e.g. Microwave Oven

DESIGN CONSIDERATION IN WLAN-SPEED/STANDARD

- 802.11a used mainly in the United Stated
- Has data rate up to 54Mbps in the 5GHz band
- Uses Orthogonal Frequency Division Multiplexing (OFDM) modulation
- 8 channels available (12 in all, 4 outdoor)

DESIGN CONSIDERATION IN WLAN-SPEED/STANDARD

- 802.11g deployed widely in Europe and Africa
- Has data rate up to 54Mbps in the 2.4GHz band
- Uses DSSS modulation extended to CCK (Complimentary Code keying)
- Supported by ETSI (European Telecommunication Standards Institute)
- Interoperable and compatible with 802.11b

DESIGN CONSIDERATION IN WLAN-COVERAGE

- The different standards discussed 802.11a,b,g have coverage limitation usually about 30m (to ensure maximum throughput)
- Also there are limited non-overlapping channel available per Access Point (AP)
- Therefore more than one Access points may be required for adequate coverage depending on the area of interest

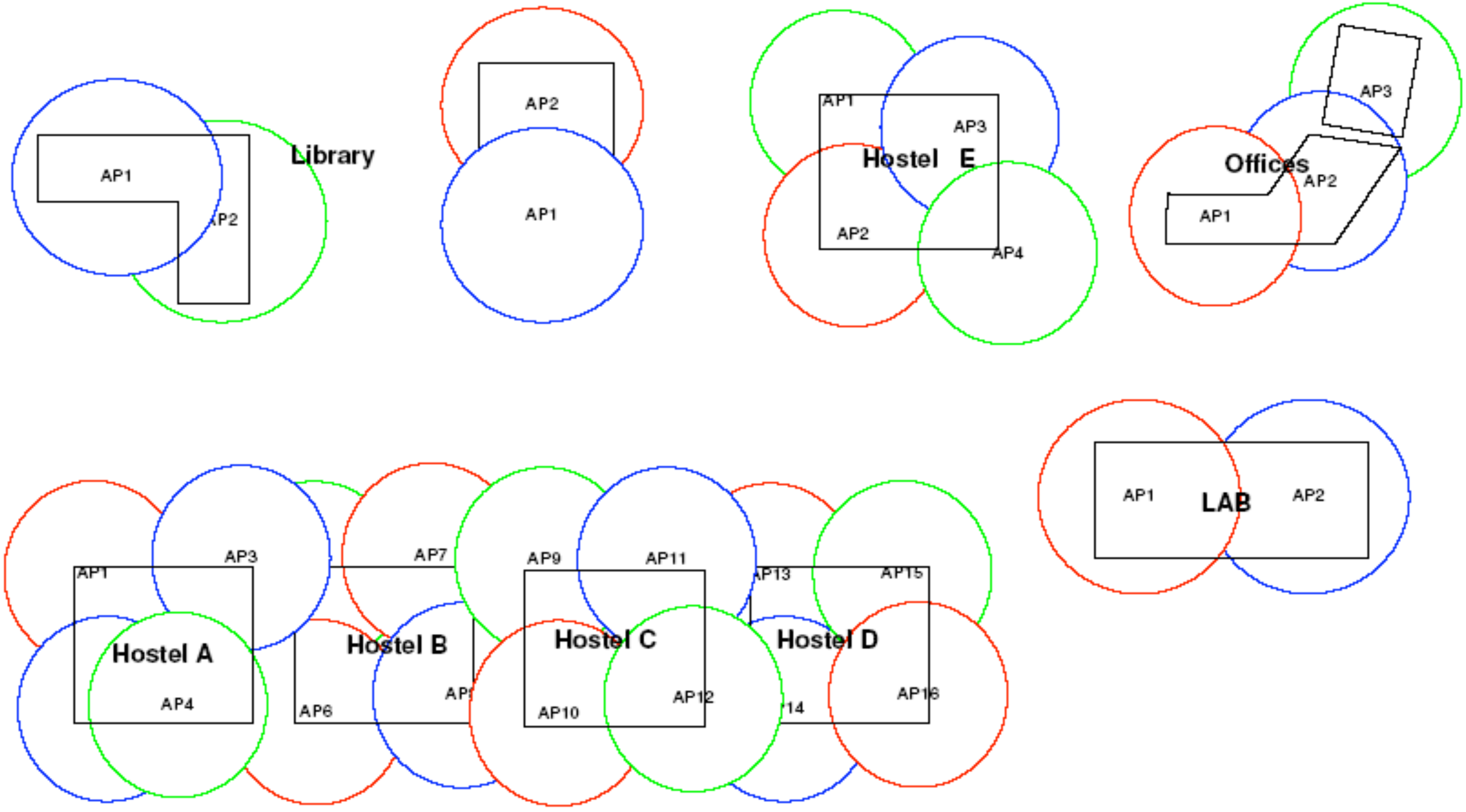


Figure 2 : Wireless Coverage and Channel Depiction

Area of coverage

DESIGN CONSIDERATION IN WLAN-DENSITY/CAPACITY

- The different standards discussed 802.11a,b,g have capacity recommendation depending on the manufacturer
- Per Access Point, the number of simultaneous end device connection could range from 10 -70 depending on the manufacturer
- Therefore more than one Access points may be required depending on the number of end-user in the area of interest

DESIGN CONSIDERATION IN WLAN-SECURITY

- This is arguably the most important area of concern for both users and designers of wireless networks
- Like all radio frequencies, anyone with a receiver can tune into a wireless channel, so you need to take extra precautions to prevent your big-eared neighbor and cybercriminals from listening in.

DESIGN CONSIDERATION IN WLAN-SECURITY

- The earliest Access Point were WEP enabled (Wired Equivalent Privacy) –WEP offers only limited security features
- WEP can be implemented in 40 or 128-bits
- WEP regulates access to a wireless network based on a computer’s hardware-specific MAC address, which is relatively simple to be sniffed out and stolen

DESIGN CONSIDERATION IN WLAN-SECURITY

- Newer APs are equipped with WPA (Wi-Fi Protected Access) which has capabilities for :Temporal Key Integrity Protocol (TKIP), EAP and its variants
  - TKIP builds on WEP and offers new encryption algorithms, and constantly changes the encryption keys making them harder for wireless hackers to capture them.
  - User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP).

DESIGN CONSIDERATION IN WLAN-POWER

- In rural areas, providing electric power for individual Access Points (APs) can be a major challenge.

- The solution proffered is to use Power over Ethernet (PoE) Switches and Access Points

DESIGN CONSIDERATION IN WLAN-RF PLANNING/MANAGEMENT

- Radio Frequency Planning in the enterprise is essential to avoid overlapping channels during AP placements.
- It is imperative to plan the RF from a centralized point – Some vendors have done a good job of this by providing RF planning and Management tools e.g. Wireless Control System (WCS)

AAUN NETWORK CASE STUDY

- Built on Centralized Wireless Design with Optical Fiber Backbone
- Fully centrally planned and Manageable
- Secure and fully integrated with Microsoft Active Directory Structure
- Based on 802.11g ,54Mbps standard with full authentication, Authorization and appropriate encryption features.

AAUN NETWORK CASE STUDY

- Has capability to support Voice, Video and Data
- Provides wireless access throughout the entire campus
- All Access Points are Lightweight and are powered via Power over Ethernet (PoE) switches

SUMMARY

Local Area Networks –wired and wireless have come to change the way we work, play and live .

Enterprises, campuses and rural educational establishments now more than ever need to tap into the vast opportunities afforded by Local Area Networks to increase efficiency, communication and have access to the unlimited amount of information and empowerment available out there.

Africa can ill afford to be left behind. Cost is no longer much of an issue as the cost of these infrastructures over the years have been driven down

Managing a Wireless LAN

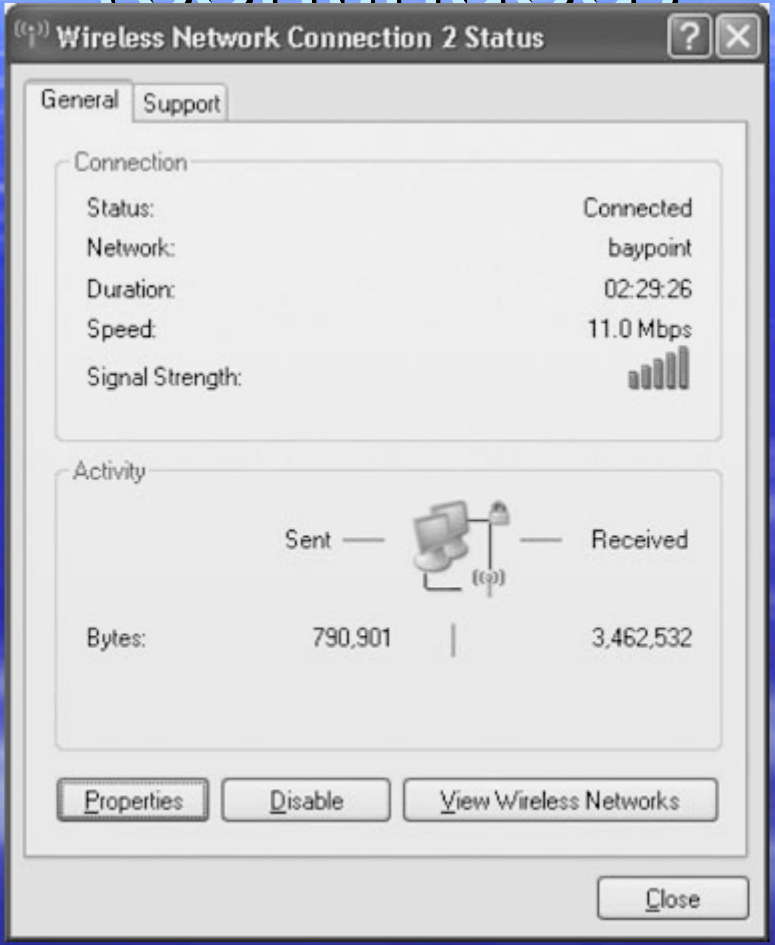
Monitoring the Wireless Network

- Network monitoring provides valuable data regarding current state of a network
  - Generate network **baseline**
  - Detect emerging problems
- Monitoring a wireless network can be performed with two sets of tools:
  - Utilities designed specifically for WLANs
  - Standard networking tools

WLAN Monitoring Tools

- Two classifications of tools:
  - Operate on wireless device itself
  - Function on AP
- **Device and Operating System Utilities:**
  - Most OSs provide basic utilities for monitoring the WLAN
  - Some vendors provide more detailed utilities
    - Often include facility to generate statistics by continually “pinging” the AP

WLAN Monitoring Tools (continued)

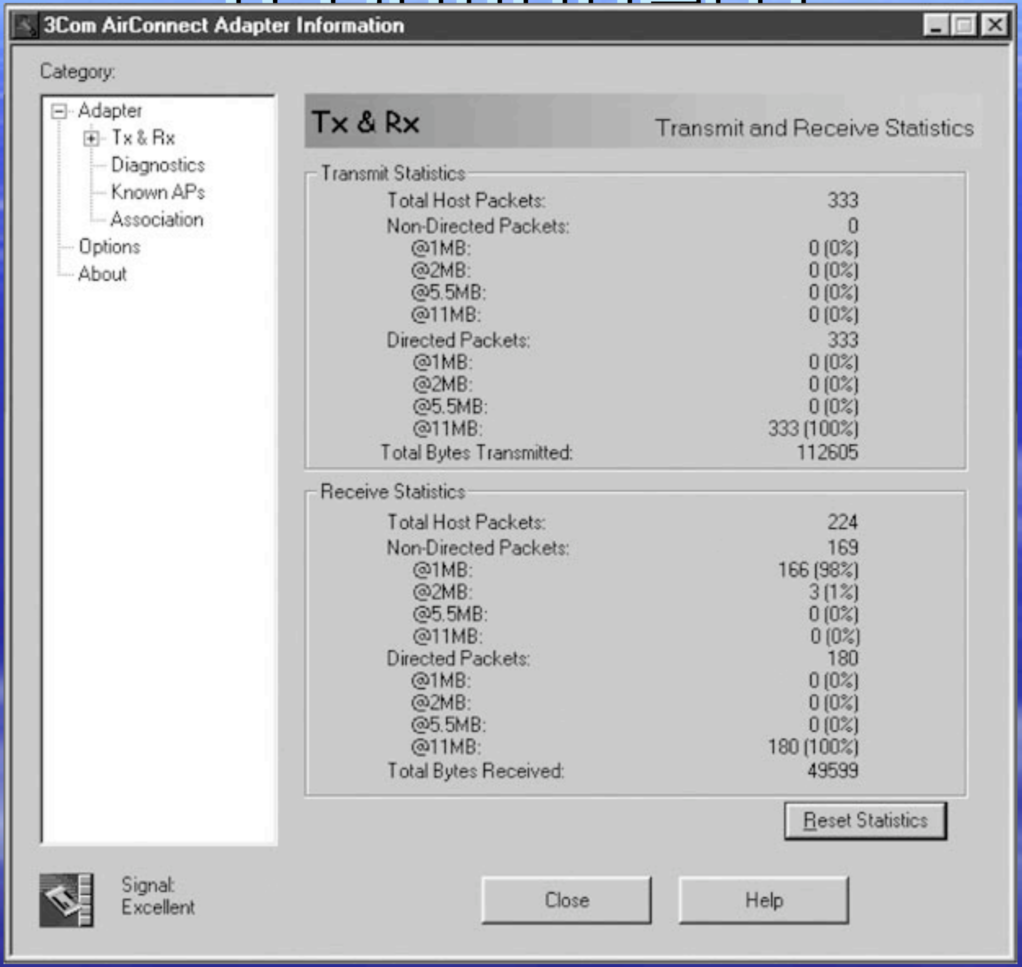


Status: Connected
Network: baypoint
Duration: 02:29:26
Speed: 11.0 Mbps
Signal Strength:

Sent — Received
Bytes: 790,901 | 3,462,532

Figure 10-1: Windows Wireless Network Connection Status

WLAN Monitoring Tools (continued)



Transmit Statistics

Total Host Packets:	333
Non-Directed Packets:	0
@1MB:	0 (0%)
@2MB:	0 (0%)
@5.5MB:	0 (0%)
@11MB:	0 (0%)
Directed Packets:	333
@1MB:	0 (0%)
@2MB:	0 (0%)
@5.5MB:	0 (0%)
@11MB:	333 (100%)
Total Bytes Transmitted:	112605

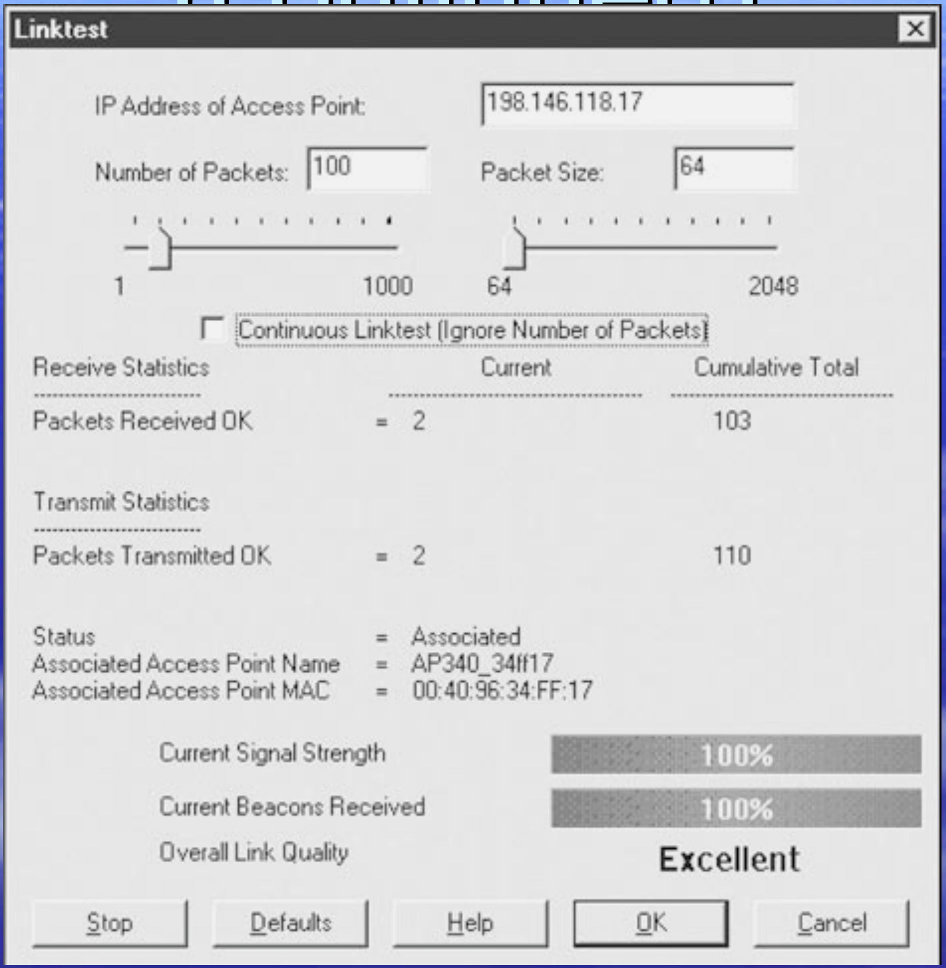
Receive Statistics

Total Host Packets:	224
Non-Directed Packets:	169
@1MB:	166 (98%)
@2MB:	3 (1%)
@5.5MB:	0 (0%)
@11MB:	0 (0%)
Directed Packets:	180
@1MB:	0 (0%)
@2MB:	0 (0%)
@5.5MB:	0 (0%)
@11MB:	180 (100%)
Total Bytes Received:	49599

Signal: Excellent

Figure 10-2: Transmit and receive statistics

WLAN Monitoring Tools (continued)



IP Address of Access Point: 198.146.118.17

Number of Packets: 100

Packet Size: 64

☐ Continuous Linktest (Ignore Number of Packets)

Receive Statistics		Current	Cumulative Total
Packets Received OK	=	2	103

Transmit Statistics		Current	Cumulative Total
Packets Transmitted OK	=	2	110

Status = Associated
Associated Access Point Name = AP340_34ff17
Associated Access Point MAC = 00:40:96:34:FF:17

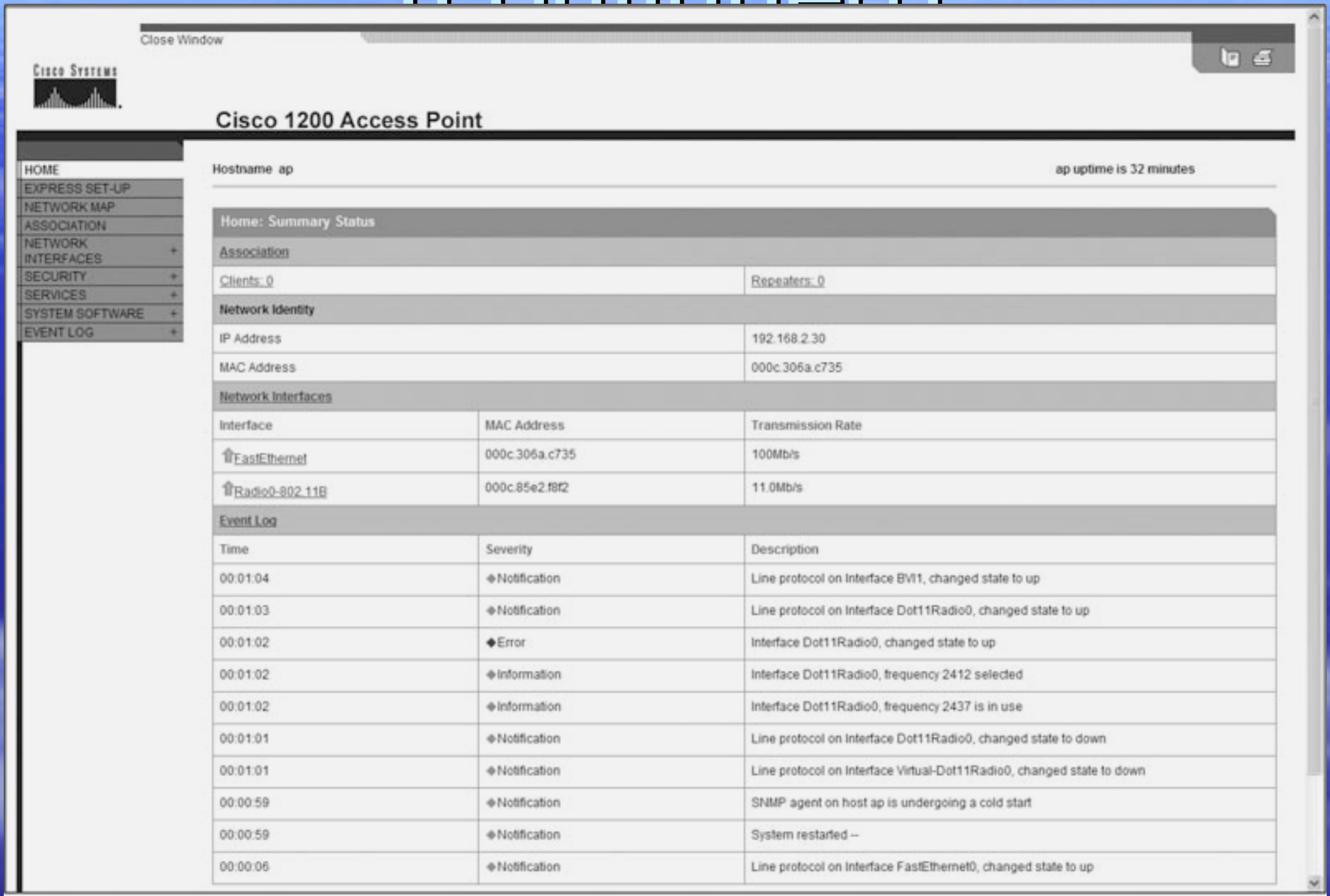
Current Signal Strength: 100%
Current Beacons Received: 100%
Overall Link Quality: **Excellent**

Figure 10-3: Testing the link

WLAN Monitoring Tools (continued)

- **Access Point Utilities**
  - All APs have WLAN reporting utilities
  - "Status" information sometimes just a summary of current AP configuration
    - No useful monitoring information
  - Many enterprise-level APs provide utilities that offer three types of information:
    - Event logs
    - Statistics on wireless transmissions
    - Information regarding connection to wired Ethernet network

WLAN Monitoring Tools (continued)



Cisco 1200 Access Point

Hostname ap

ap uptime is 32 minutes

Home: Summary Status

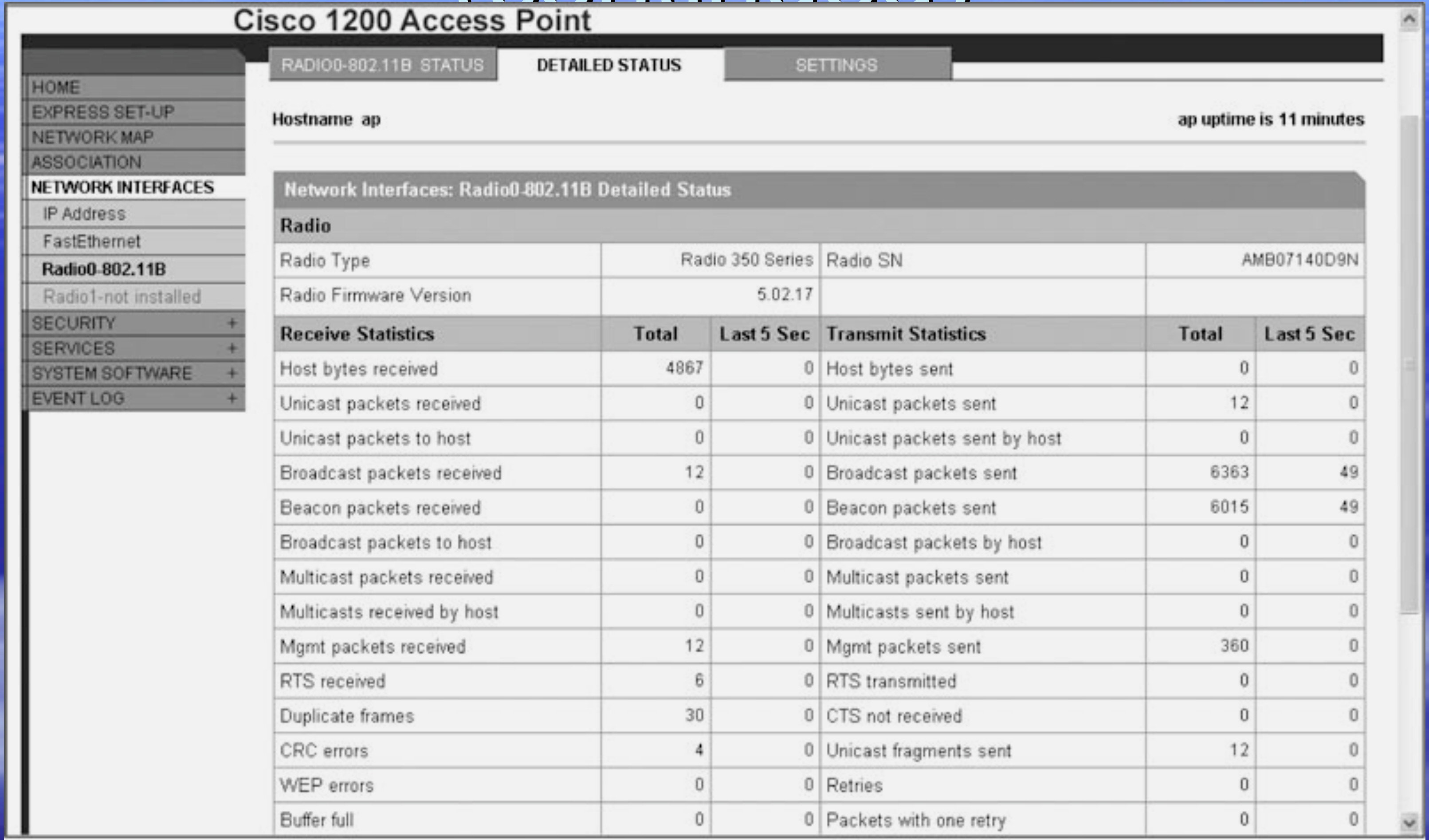
Association	
Clients: 0	Repeaters: 0
Network Identity	
IP Address	192.168.2.30
MAC Address	000c.306a.c735

Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	000c.306a.c735	100Mb/s
Radio0-802.11B	000c.85e2.f8f2	11.0Mb/s

Event Log		
Time	Severity	Description
00:01:04	◆Notification	Line protocol on Interface BVI1, changed state to up
00:01:03	◆Notification	Line protocol on Interface Dot11Radio0, changed state to up
00:01:02	◆Error	Interface Dot11Radio0, changed state to up
00:01:02	◆Information	Interface Dot11Radio0, frequency 2412 selected
00:01:02	◆Information	Interface Dot11Radio0, frequency 2437 is in use
00:01:01	◆Notification	Line protocol on Interface Dot11Radio0, changed state to down
00:01:01	◆Notification	Line protocol on Interface Virtual-Dot11Radio0, changed state to down
00:00:59	◆Notification	SNMP agent on host ap is undergoing a cold start
00:00:59	◆Notification	System restarted --
00:00:06	◆Notification	Line protocol on Interface FastEthernet0, changed state to up

Figure 10-5: Access point event log

WLAN Monitoring Tools (continued)



Hostname ap

ap uptime is 11 minutes

Network Interfaces: Radio0-802.11B Detailed Status

Radio

Radio Type	Radio 350 Series	Radio SN	AMB07140D9N
Radio Firmware Version	5.02.17		

Receive Statistics	Total	Last 5 Sec	Transmit Statistics	Total	Last 5 Sec
Host bytes received	4867	0	Host bytes sent	0	0
Unicast packets received	0	0	Unicast packets sent	12	0
Unicast packets to host	0	0	Unicast packets sent by host	0	0
Broadcast packets received	12	0	Broadcast packets sent	6363	49
Beacon packets received	0	0	Beacon packets sent	6015	49
Broadcast packets to host	0	0	Broadcast packets by host	0	0
Multicast packets received	0	0	Multicast packets sent	0	0
Multicasts received by host	0	0	Multicasts sent by host	0	0
Mgmt packets received	12	0	Mgmt packets sent	360	0
RTS received	6	0	RTS transmitted	0	0
Duplicate frames	30	0	CTS not received	0	0
CRC errors	4	0	Unicast fragments sent	12	0
WEP errors	0	0	Retries	0	0
Buffer full	0	0	Packets with one retry	0	0

Figure 10-6: Access point wireless transmissions

Standard Network Monitoring Tools

- Drawbacks to relying solely on info from AP and wireless devices:
  - Lack of Retention of data
  - Laborious and time-intensive data collection
  - Data generally not collected in time manner
- "Standard" network monitoring tools:
  - Used on wired networks
  - Proven to be reliable
  - **Simple Network Management Protocol (SNMP)**

Simple Network Management Protocol (SNMP)

- Protocol allowing computers and network equipment to gather data about network performance
  - Part of TCP/IP protocol suite
- **Software agent** loaded onto each network device that will be managed using SNMP
  - Monitors network traffic and stores info in **management information base (MIB)**
  - **SNMP management station:** Computer with the SNMP management software

Simple Network Management Protocol (continued)

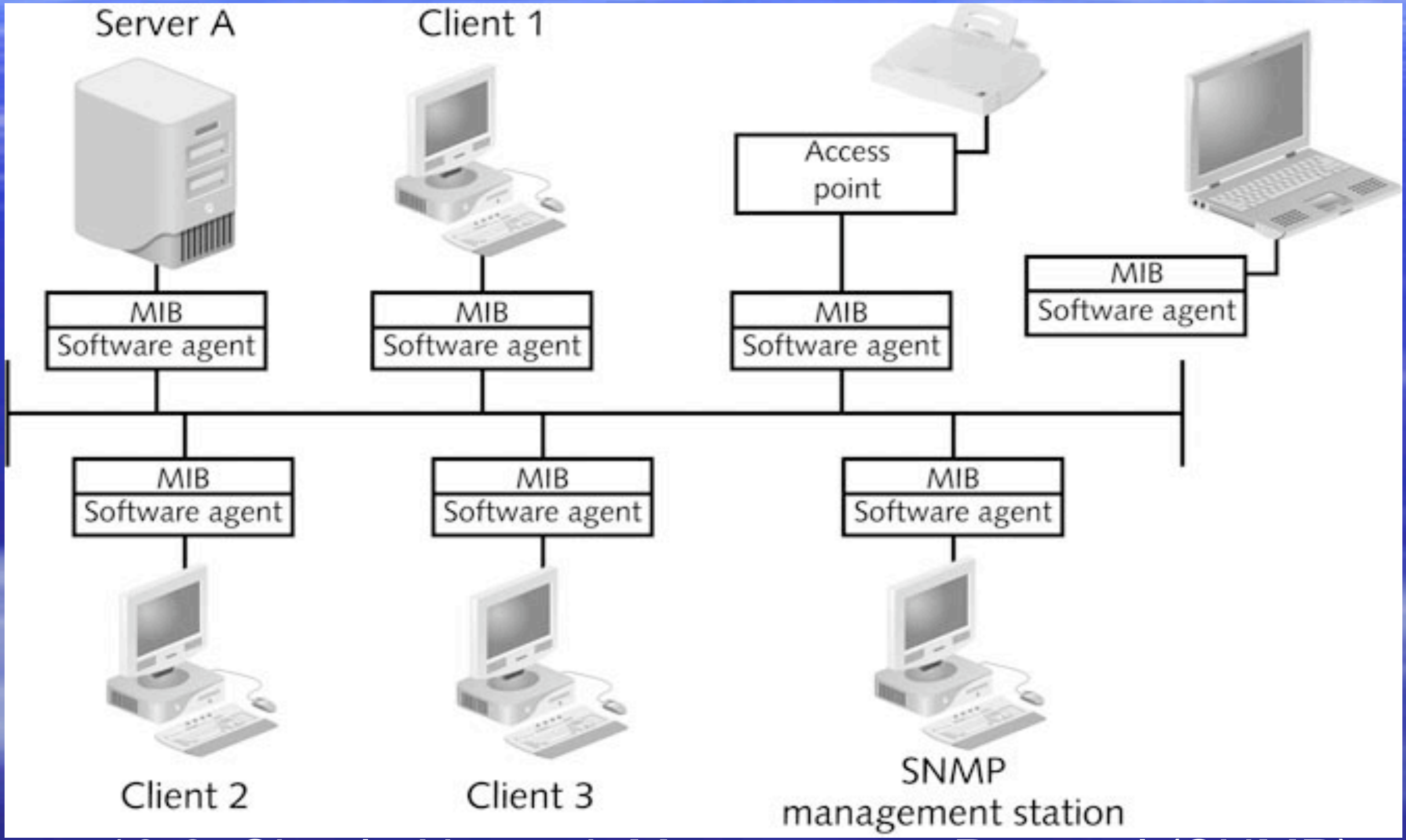
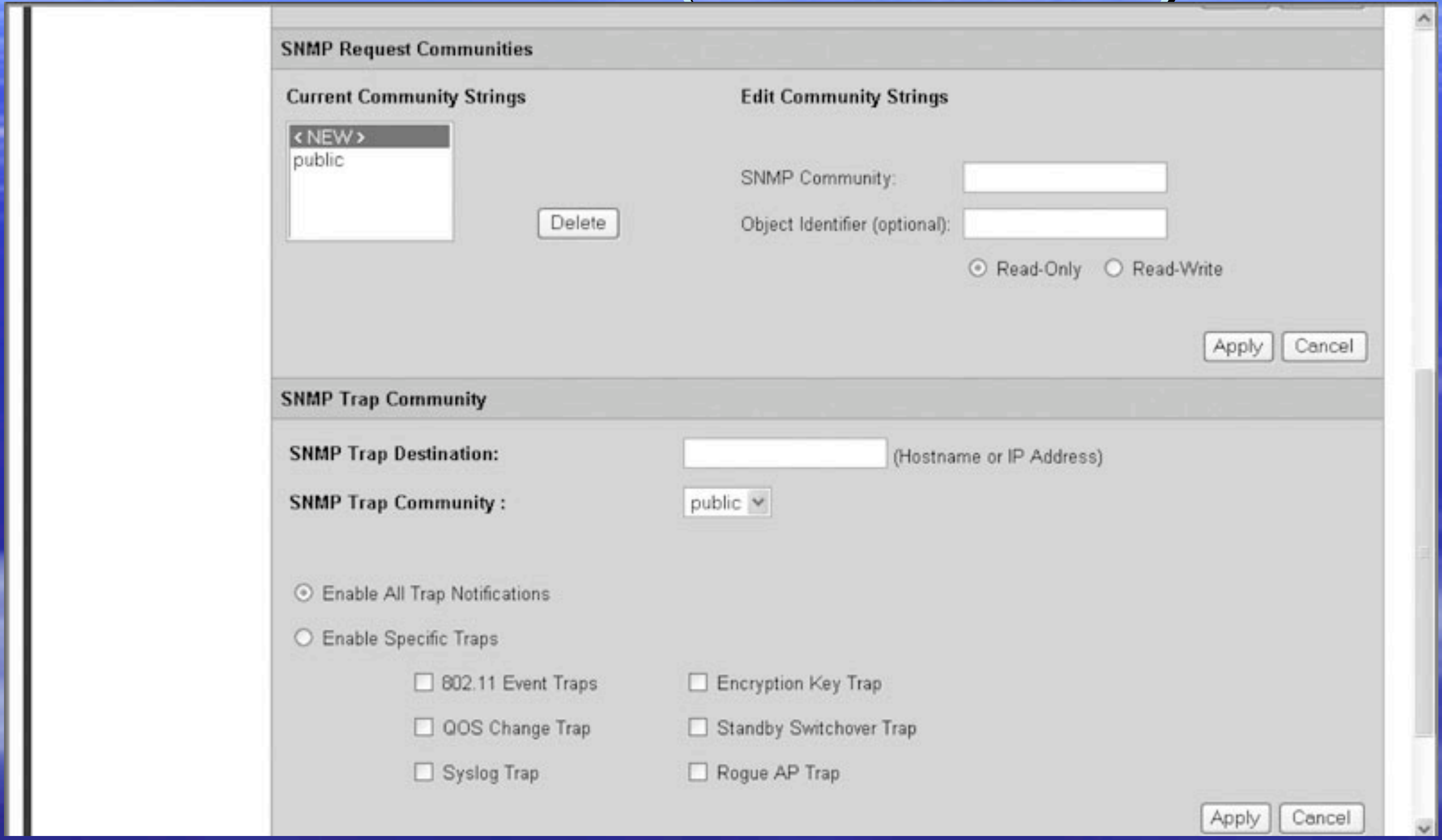


Figure 10-8: Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (continued)

- SNMP management station communicates with software agents on network devices
  - Collects data stored in MIBs
  - Combines and produces statistics about network
- Whenever network exceeds predefined limit, triggers an **SNMP trap**
  - Sent to management station
- Implementing SNMP provides means to acquire wireless data for establishing

Simple Network Management Protocol (continued)



SNMP Request Communities

Current Community Strings

< NEW >
public

Edit Community Strings

SNMP Community:
Object Identifier (optional):
● Read-Only ○ Read-Write

SNMP Trap Community

SNMP Trap Destination: (Hostname or IP Address)
SNMP Trap Community : public

● Enable All Trap Notifications
○ Enable Specific Traps
☐ 802.11 Event Traps
☐ QOS Change Trap
☐ Syslog Trap
☐ Encryption Key Trap
☐ Standby Switchover Trap
☐ Rogue AP Trap

Figure 10-10: Cisco SNMP traps

Remote Monitoring (RMON)

- SNMP-based tool used to monitor LANs connected via a **wide area network (WAN)**
  - WANs provide communication over larger geographical area than LANs
- Allows remote network node to gather network data at almost any point on a LAN or WAN
  - Uses SNMP and incorporates special database for remote monitoring
- WLAN AP can be monitored using RMON

Maintaining the Wireless Network

- Wireless networks are not static
  - Must continually be modified, adjusted, and tweaked
- Modifications often made in response to data gathered during network monitoring
- Two of most common functions:
  - Updating AP firmware
  - Adjusting antennas to enhance transmissions

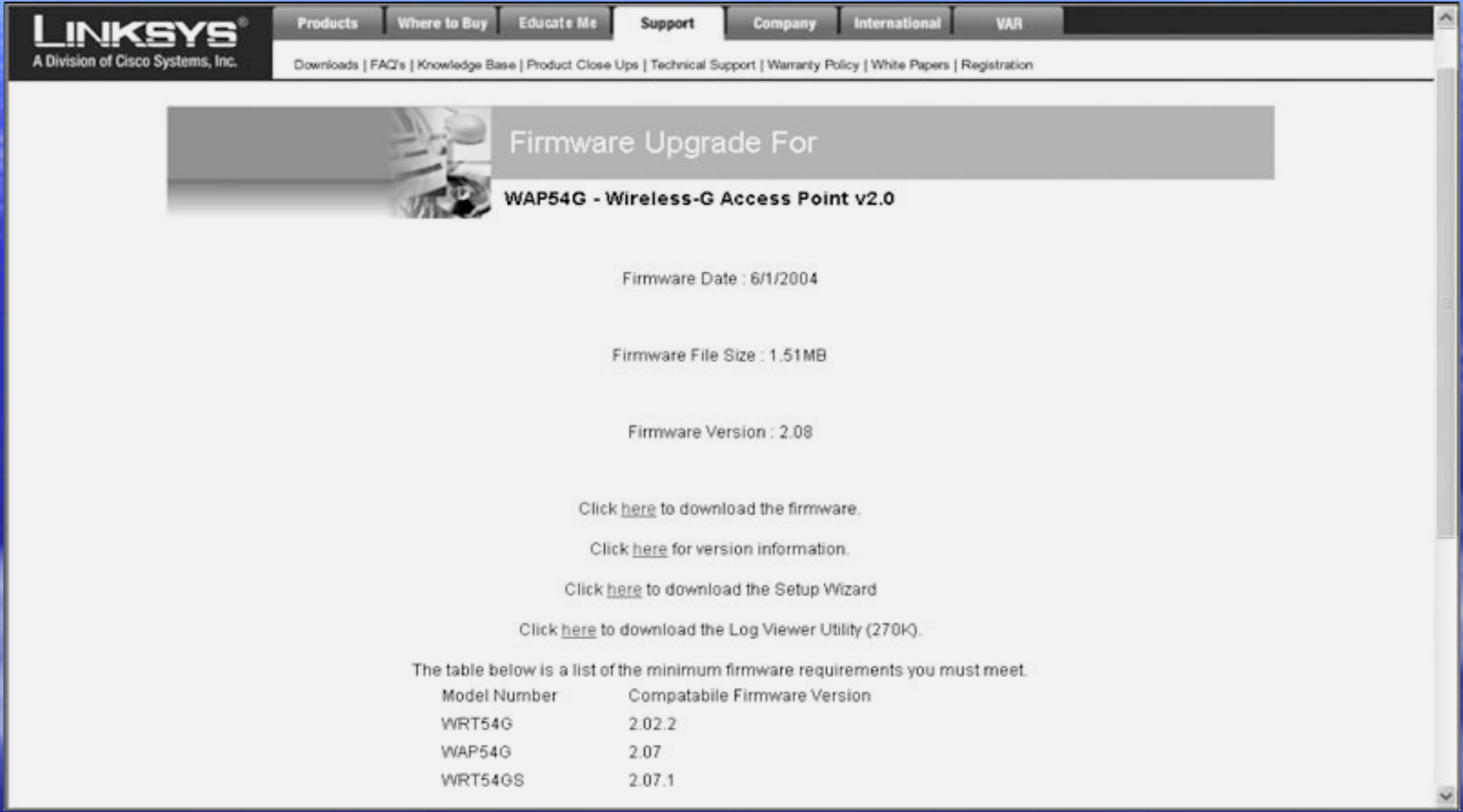
Upgrading Firmware

- **Firmware**: Software embedded into hardware to control the device
  - – Electronic “heart” of a hardware device
  - – Resides on **EEPROM**
    - Nonvolatile storage chip
- Most APs use a browser-based management system
- Keep APs current with latest changes by downloading the changes to the APs

Upgrading Firmware (continued)

- General steps to update AP firmware:
  - Download firmware from vendor’s Web site
  - Select “Upgrade Firmware” or similar option from AP
  - Enter location of firmware file
  - Click *Upgrade* button
- Enterprise-level APs often have enhanced firmware update capabilities
  - e.g., may be able to update System firmware, Web Page firmware, and Radio firmware separately

Upgrading Firmware (continued)


LINKSYS®
A Division of Cisco Systems, Inc.
Products
Where to Buy
Educate Me
Support
Company
International
VAR
Downloads | FAQ's | Knowledge Base | Product Close Ups | Technical Support | Warranty Policy | White Papers | Registration

Firmware Upgrade For

WAP54G - Wireless-G Access Point v2.0

Firmware Date : 6/1/2004

Firmware File Size : 1.51MB

Firmware Version : 2.08

Click here to download the firmware.

Click here for version information.

Click here to download the Setup Wizard

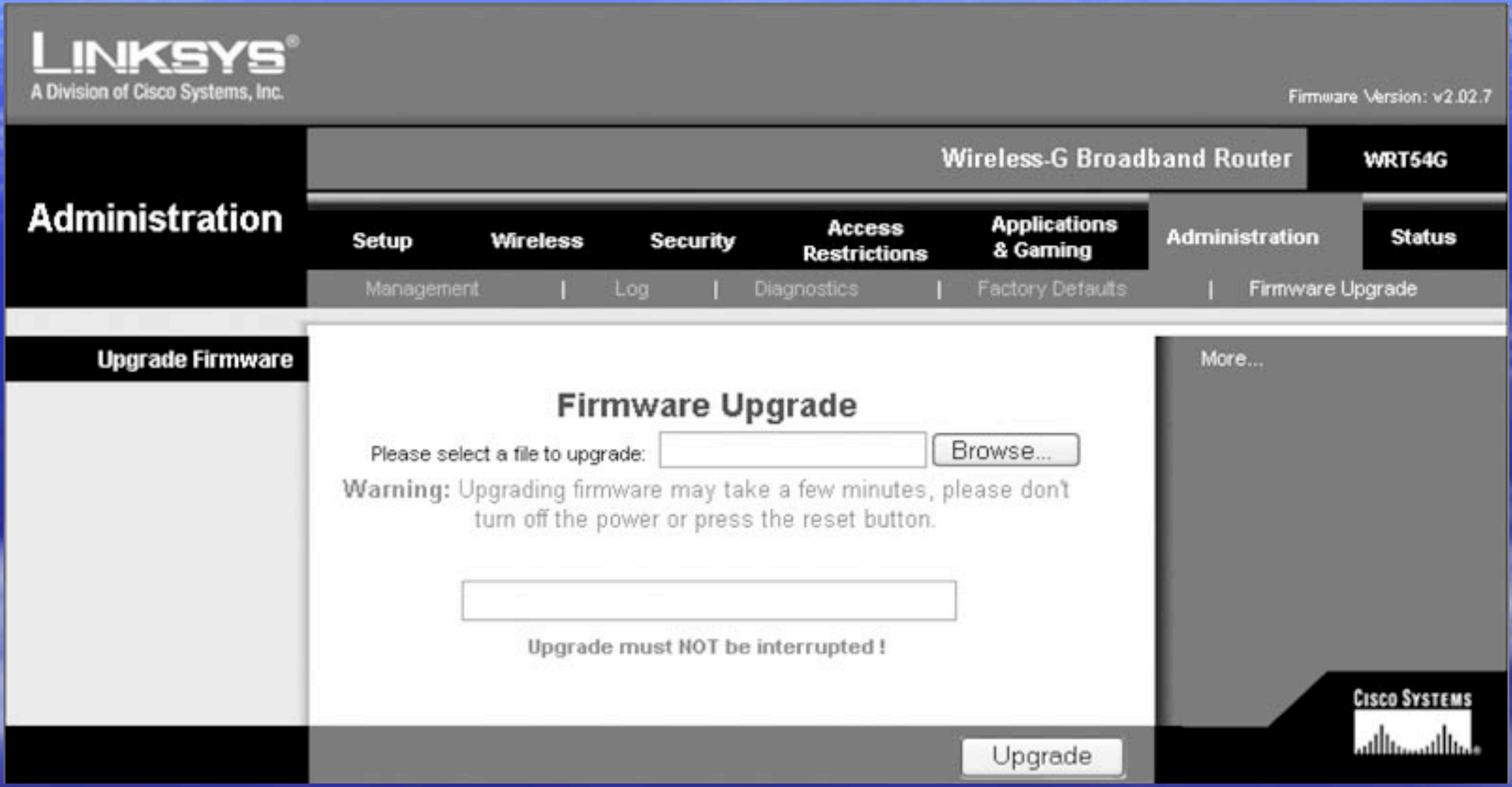
Click here to download the Log Viewer Utility (270K).

The table below is a list of the minimum firmware requirements you must meet.

Model Number	Compatabile Firmware Version
WRT54G	2.02.2
WAP54G	2.07
WRT54GS	2.07.1

Figure 10-11: Internet firmware update page

Upgrading Firmware (continued)



Firmware Upgrade

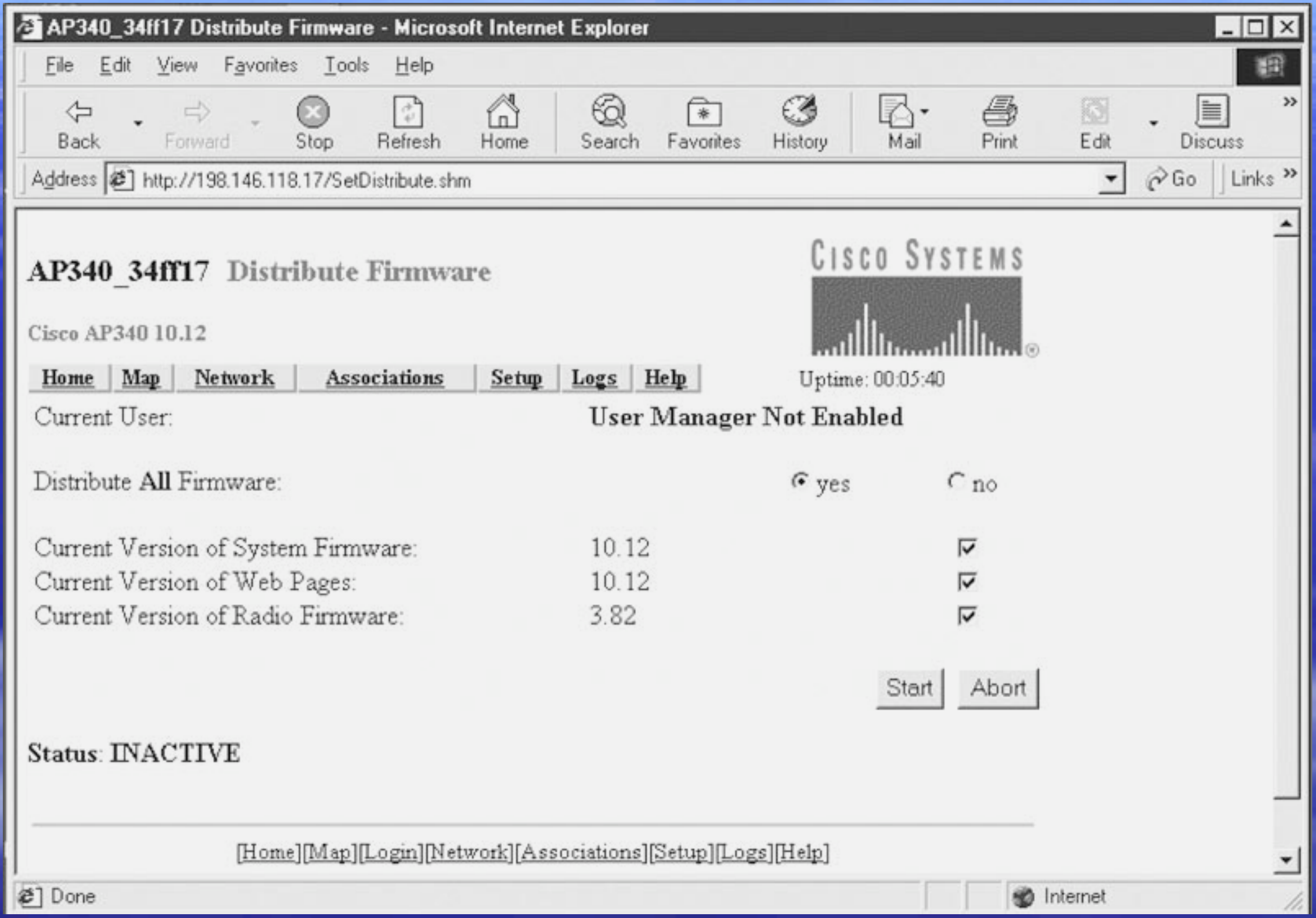
Please select a file to upgrade:

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted !

Figure 10-12: AP firmware update page

Upgrading Firmware (continued)



AP340_34ff17 Distribute Firmware - Microsoft Internet Explorer

Address http://198.146.118.17/SetDistribute.shm

AP340_34ff17 Distribute Firmware

Cisco AP340 10.12

File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Go Links
Cisco Systems
Home | Map | Network | Associations | Setup | Logs | Help
Start
Abort
[Home][Map][Login][Network][Associations][Setup][Logs][Help]
Done
Internet

Uptime: 00:05:40

Current User: **User Manager Not Enabled**

Distribute All Firmware: ● yes ○ no

Current Version of System Firmware: 10.12 ☑

Current Version of Web Pages: 10.12 ☑

Current Version of Radio Firmware: 3.82 ☑

Status: INACTIVE

Figure 10-13: Separate firmware updates

Upgrading Firmware (continued)

- With many enterprise-level APs, once a single AP has been upgraded to the latest firmware, can distribute to all other APs on the WLAN
  - – Receiving AP must be able to hear IP multicast issued by Distribution AP
  - – Receiving AP must be set to allow access through a Web browser
  - – If Receiving AP has specific security capabilities enabled, must contain in its approved user lists a user with the same user name, password, and

Upgrading Firmware (continued)

- **RF site tuning:** After firmware updates applied, adjusting APs' setting
  - – Adjust radio power levels on all access points
    - Firmware upgrades may increase RF coverage areas
  - – Adjust channel settings
  - – Validate coverage area
  - – Modify integrity and throughput
  - – Document changes

Adjusting Antennas: RF Transmissions

- May need to adjust antennas in response to firmware upgrades or changes in environment
  - May require reorientation or repositioning
  - May require new type of antenna
- Radio frequency link between sender and receiver consists of three basic elements:
  - Effective transmitting power
  - Propagation loss
  - Effective receiving sensibility

Adjusting Antennas: RF Transmissions (continued)

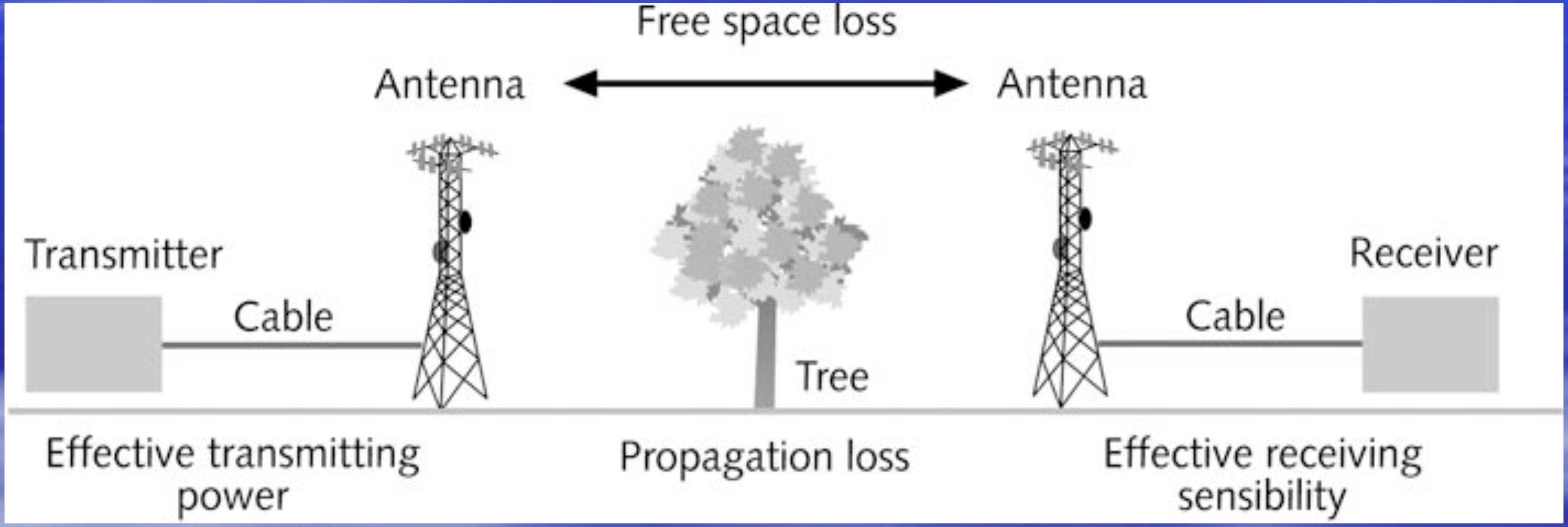


Figure 10-14: Radio frequency link

Adjusting Antennas: RF Transmissions (continued)

- **Link budget:** Calculation to determine if signal will have proper strength when it reaches link's end
  - Required information:
    - Antenna gain
    - Free space path loss
    - Frequency of the link
    - Loss of each connector at the specified frequency
    - Number of connectors used
    - Path length
    - Power of the transmitter

Adjusting Antennas: RF Transmissions (continued)

- **Link budget (continued):**
  - Required information (continued):
    - Total length of transmission cable and loss per unit length at specified frequency
- For proper WLAN performance, link budget must be greater than zero
  - **System operating margin (SOM)**
  - Good WLAN link has link budget over 6 dB
  - **Fade margin:** Difference between strongest RF signal in an area and weakest signal that a receiver can process

Adjusting Antennas: RF Transmissions (continued)

- **Attenuation (loss):** Negative difference in amplitude between RF signals
  - Absorption
  - Reflection
  - Scattering
  - Refraction
  - Diffraction
  - Voltage Standing Wave Ratio

Adjusting Antennas: Antenna Types

- **Rod antenna:** Antenna typically used on a WLAN
  - Omnidirectional
  - 360 degree radiation pattern
  - Transmission pattern focused along horizontal plane
  - Increasing length creates “tighter” 360-degree beam
- **Sectorized antenna:** “Cuts” standard 360-degree pattern into four quarters

Adjusting Antennas: Antenna Types (continued)

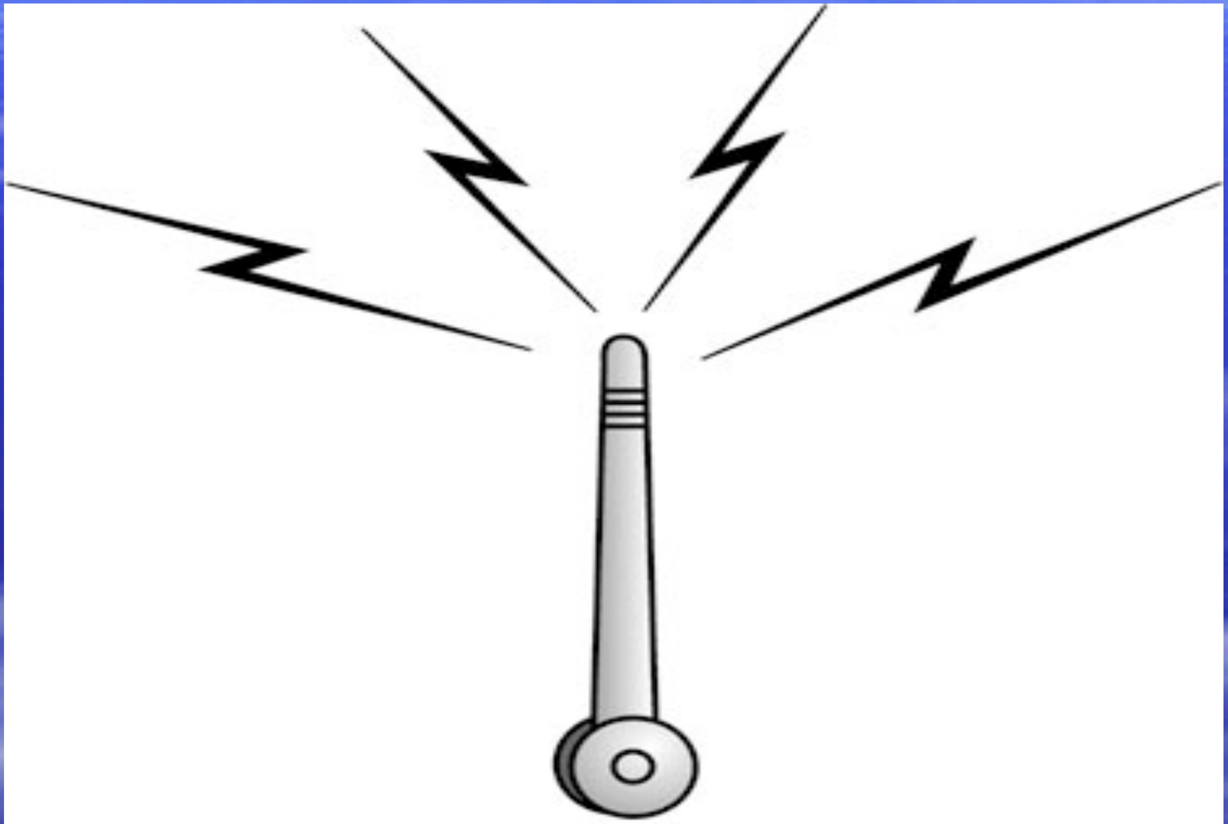


Figure 10-15: Rod antenna pattern

Adjusting Antennas: Antenna Types (continued)

- **Panel antenna:** Typically used in outdoor areas
  - "Tight" beamwidth
- **Phase shifter:** Allows wireless device to use a **beam steering antenna** to improve receiver performance
  - Direct transmit antenna pattern to target
- **Phased array antenna:** Incorporates network of phase shifters, allowing antenna to be pointed electronically in microseconds,

Adjusting Antennas: Antenna Types (continued)

- Radiation pattern emitting from antennas travels in three-dimensional “donut” form
  - **Azimuth and elevation** planes
- **Antenna Accessories:**
  - Transmission problem can be resolved by adding “accessories” to antenna system
  - Provide additional power to the antenna, decrease power when necessary, or provide additional functionality

Adjusting Antennas: Antenna Types (continued)

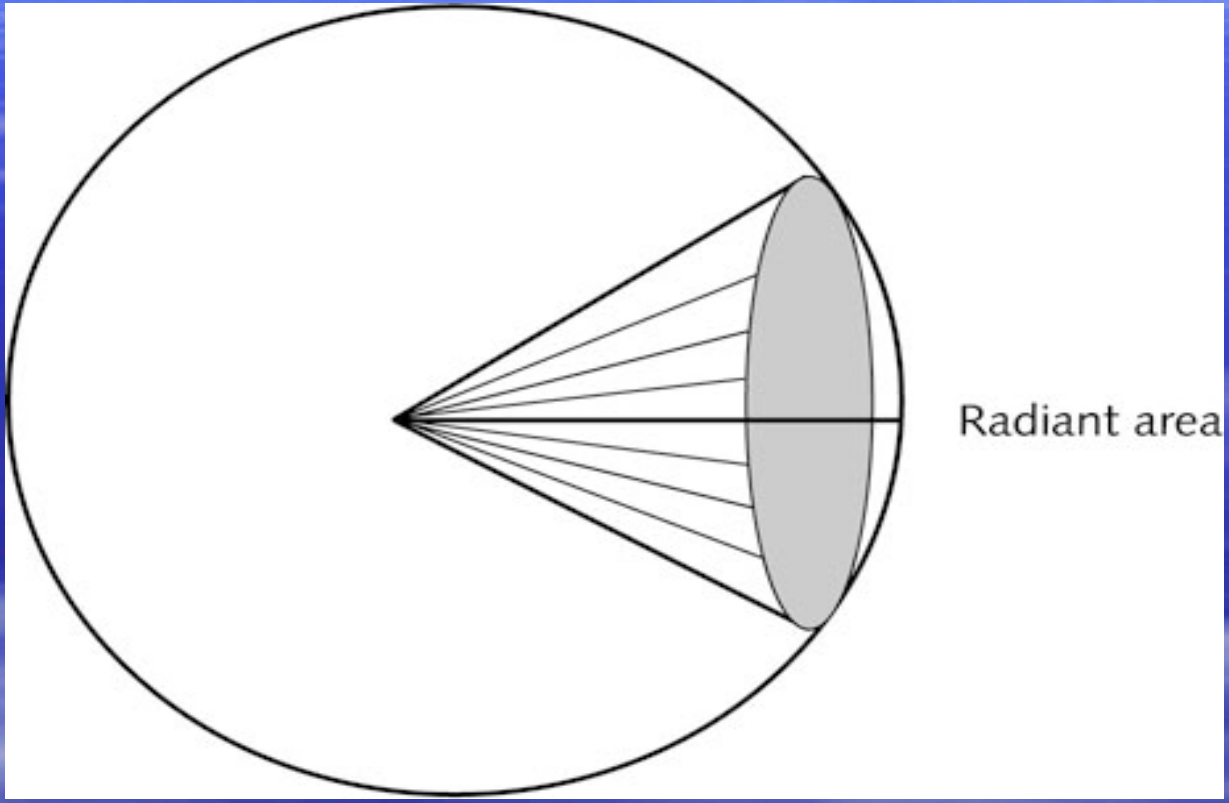


Figure 10-17: Azimuth and elevation pattern

Adjusting Antennas: RF Amplifier

- Increases amplitude of an RF signal
  - **Signal gain**
- **Unidirectional amplifier:** Increases RF signal level before injected into transmitting antenna
- **Bidirectional amplifier:** Boosts RF signal before injected into device containing the antenna
  - Most amplifiers for APs are bidirectional

Adjusting Antennas: RF Attenuators

- Decrease RF signal
  - May be used when gain of an antenna did not match power output of an AP
- **Fixed-loss attenuators:** Limit RF power by set amount
- **Variable-loss attenuators:** Allow user to set amount of loss
- Fixed-loss attenuators are the only type permitted by the FCC for WLAN systems

Adjusting Antennas: Cables and Connectors

- Basic rules for selecting cables and connectors:
  - Ensure connector matches electrical capacity of cable and device, along with type and gender of connector
  - Use high-quality connectors and cables
  - Make cable lengths as short as possible
  - Make sure cables match electrical capacity of connectors
  - Try to purchase pre-manufactured cables
  - Use splitters sparingly

Adjusting Antennas: Lightning Arrestor

- Antennas can inadvertently pick up high electrical discharges
  - From nearby lightning strike or contact with high-voltage electrical source
- **Lightning Arrestor:** Limits amplitude and disturbing interference voltages by channeling them to ground
  - Designed to be installed between antenna cable and wireless device
    - One end (3) connects to antenna
    - Other end (2) connects to wireless device
    - Ground lug (1) connects to grounded cable

Adjusting Antennas: Lightning Arrestor (continued)

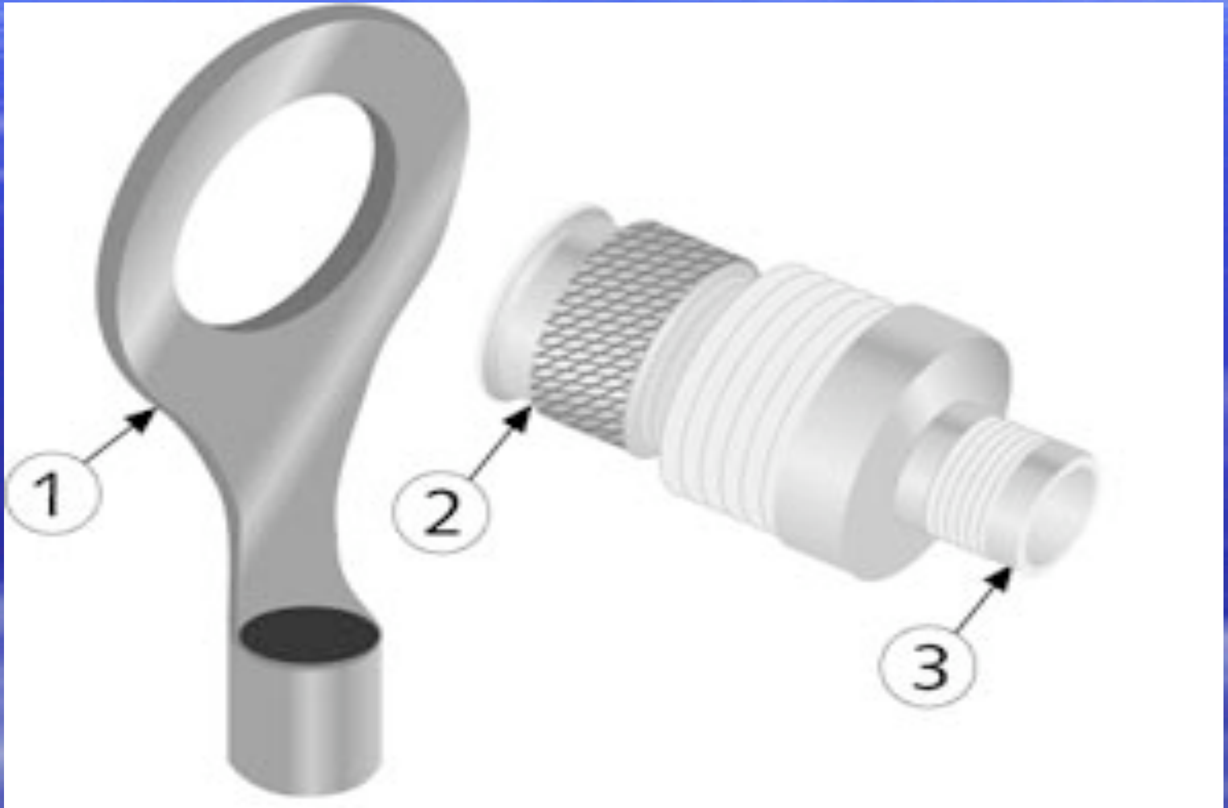


Figure 10-18: Lightning arrestor

Establishing a Wireless Security Policy

- One of most important acts in managing a WLAN
  - – Should be backbone of any wireless network
  - – Without it, no effective wireless security

General Security Policy Elements

- **Security policy:** Document or series of documents clearly defining the defense mechanisms an organization will employ to keep information secure
  - Outlines how to respond to attacks and information security duties/responsibilities of employees
- Three key elements:
  - Risk assessment
  - Security auditing

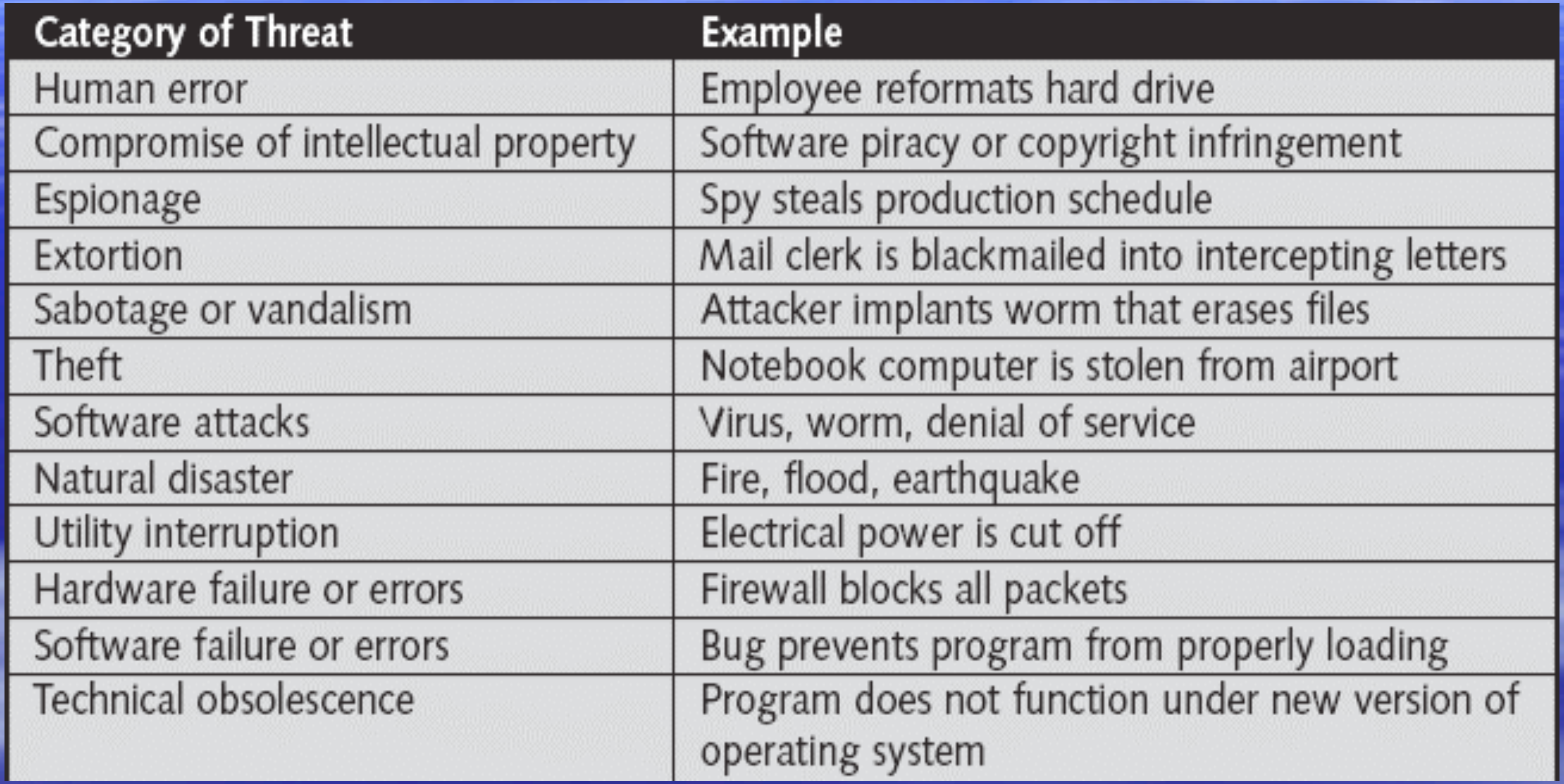
Risk Assessment

- Determine nature of risks to organization's assets
  - First step in creating security policy
- **Asset:** Any item with positive economic value
  - Physical assets
  - Data
  - Software
  - Hardware
  - Personnel

Risk Assessment (continued)

- Factors to consider in determining relative value:
  - How critical is this asset to the goals of the organization?
  - How much profit does it generate?
  - How much revenue does it generate?
  - What is the cost to replace it?
  - How much does it cost to protect it?
  - How difficult would it be to replace it?
  - How quickly can it be replaced?
  - What is the security impact if this asset is

Risk Assessment (continued)



Category of Threat	Example
Human error	Employee reformats hard drive
Compromise of intellectual property	Software piracy or copyright infringement
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Sabotage or vandalism	Attacker implants worm that erases files
Theft	Notebook computer is stolen from airport
Software attacks	Virus, worm, denial of service
Natural disaster	Fire, flood, earthquake
Utility interruption	Electrical power is cut off
Hardware failure or errors	Firewall blocks all packets
Software failure or errors	Bug prevents program from properly loading
Technical obsolescence	Program does not function under new version of operating system

Table 10-1: Threats to information security

Security Auditing

- Determining what current security weaknesses may expose assets to threats
  - Takes current snapshot of wireless security of organization
- Each threat may reveal multiple vulnerabilities
- **Vulnerability scanners:** Tools that can compare an asset against database of known vulnerabilities
  - Produce discovery report that exposes the

Impact Analysis

- Involves determining likelihood that vulnerability is a risk to organization
- Each vulnerability can be ranked:
  - No impact
  - Small impact
  - Significant
  - Major
  - Catastrophic
- Next, estimate probability that vulnerability will actually occur
  - Rank on scale of 1 to 10

Impact Analysis (continued)

- Final step is to determine what to do about risks
  - – Accept the risk
  - – Diminish the risk
  - – Transfer the risk
- Desirable to diminish all risks to some degree
  - – If not possible, risks for most important assets should be reduced first

Functional Security Policy Elements

- **Baseline practices:** Establish benchmark for actions using wireless network
  - Can be used for creating **design and implementation practices**
    - Foundation of what conduct is acceptable on the WLAN
- Security policy must specifically identify **physical security**
  - Prevent unauthorized users from reaching equipment in order to use, steal, or vandalize it

Functional Security Policy Elements (continued)

- **Social engineering:** Relies on tricking or deceiving someone to access a system
  - – Best defeated in two ways:
    - Develop strong procedures/policies regarding when passwords are given out, who can enter premises, and what to do when asked questions by another employee that may reveal protected information
    - Educating all employees about policies and ensuring they are followed

Tutorial On Implementing and Managing Networks

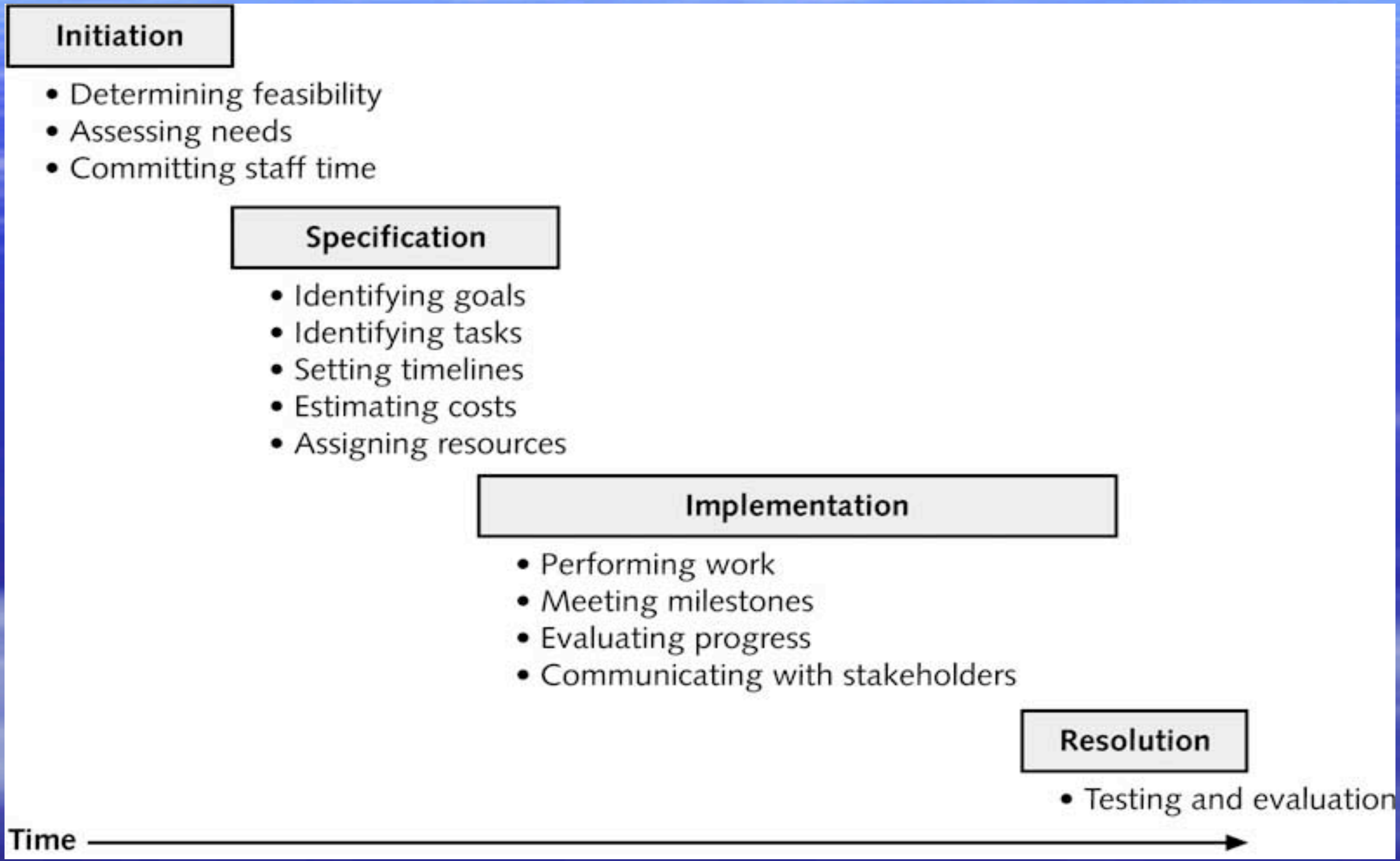
Project Management

- Managing staff, budget, timelines, and other resources and variables to achieve specific goal within given bounds
- Attempts to answer at least following questions:
  - Is proposed project feasible?
  - What needs must project address?
  - What are project's goals?
  - What tasks are required to meet goals?
  - How long should tasks take, and in what order

Project Management (continued)

- Attempts to answer at least the following questions (continued):
  - What resources are required, and how much will they cost?
  - Who will be involved and what skills are needed?
  - How will staff communicate?
  - After completion, did project meet stated need?
- Most projects divided into phases
- Milestone: reference point marking

Project Management (continued)



Initiation

- Determining feasibility
- Assessing needs
- Committing staff time

Specification

- Identifying goals
- Identifying tasks
- Setting timelines
- Estimating costs
- Assigning resources

Implementation

- Performing work
- Meeting milestones
- Evaluating progress
- Communicating with stakeholders

Resolution

- Testing and evaluation

Figure 15-1: Project phases

Determining Project Feasibility

- Feasibility study outlines costs and benefits of project
  - Attempts to predict whether it will yield favorable outcome
  - Should be performed for any large-scale project before resources committed

Assessing Needs

- Needs assessment: process of clarifying reasons and objectives underlying proposed change(s)
  - Interviewing users
  - Comparing perceptions to factual data
  - Analyzing network baseline data

Assessing Needs (continued)

- Needs assessment may address the following:
  - Is expressed need valid or does it mask a different need?
  - Can need be resolved?
  - Is need important enough to allocate resources to its resolution? Will meeting it have measurable effect on productivity?
  - If fulfilled, will need result in additional needs? Will fulfilling it satisfy other needs?
  - Do users affected by the need agree that change is a good answer? What kind of resolution will satisfy them?

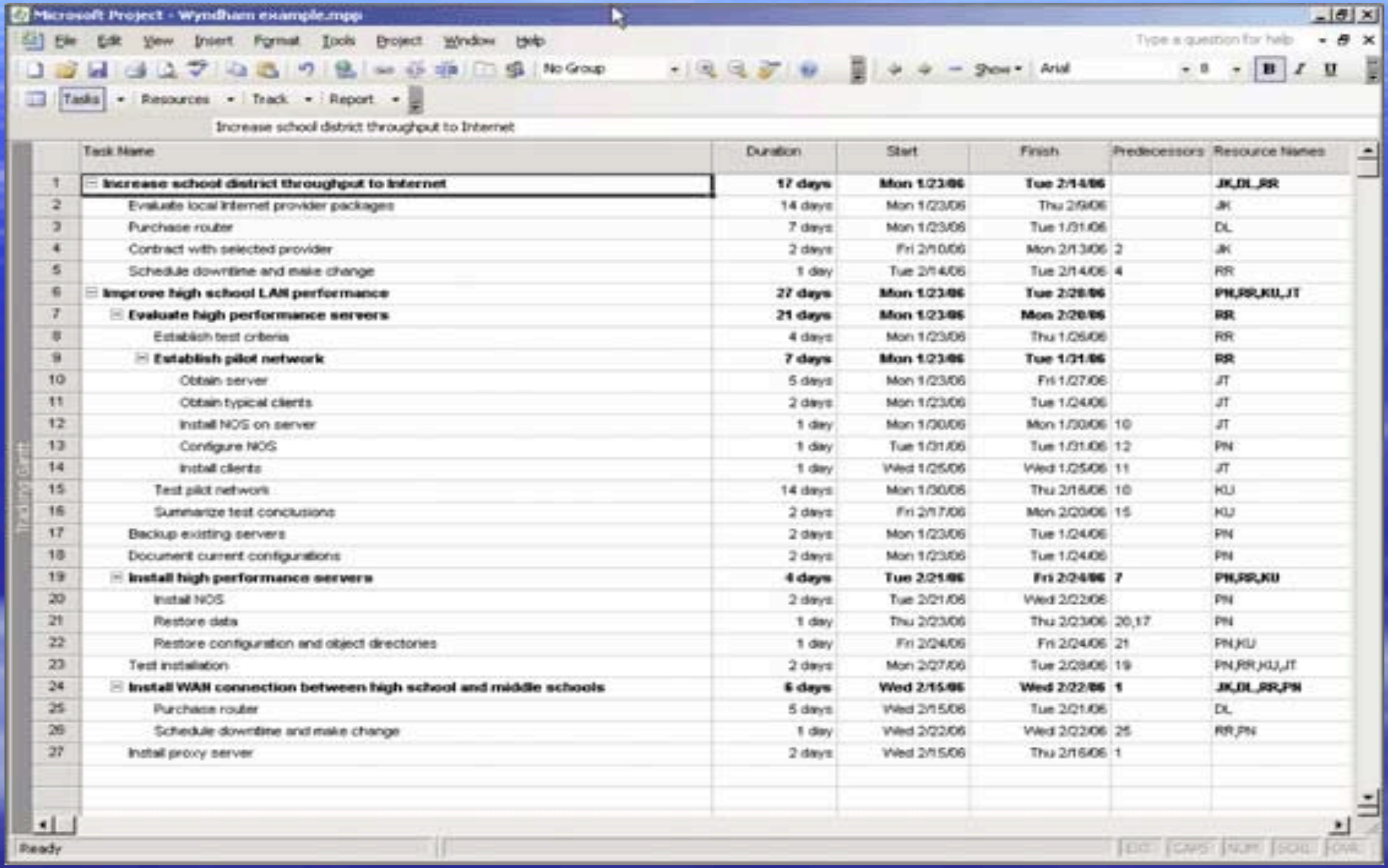
Setting Project Goals

- Project goals help keep project on track
  - Necessary when evaluating whether project was successful
- Popular technique is to begin with broad goal, narrow down to specific sub-goals
- Project goals should be attainable
  - Feasibility study helps determine attainability
- Sponsors: managers and others who oversee resource allocation
- Stakeholder: any person affected by the

Project Planning

- Project plan: organizes details of a project
  - – e.g., timeline and significant tasks
  - – May use text or spreadsheet documents for small projects
  - – For large projects, use project management software
    - Provides framework for inputting tasks, timelines, resource assignments, completion dates, and so on

Project Planning (continued)


Microsoft Project - Wyndham example.mpp
File Edit View Insert Format Tools Project Window Help
Type a question for help
No Group
Show
Arial
8
B I U
Tasks Resources Track Report
Gantt Chart
Ready
EXT CAPS NUM SCRL OVR

Increase school district throughput to Internet

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Increase school district throughput to Internet**	**17 days**	**Mon 1/23/06**	**Tue 2/14/06**		**JK,DL,RR**
2	Evaluate local Internet provider packages	14 days	Mon 1/23/06	Thu 2/9/06		JK
3	Purchase router	7 days	Mon 1/23/06	Tue 1/31/06		DL
4	Contract with selected provider	2 days	Fri 2/10/06	Mon 2/13/06	2	JK
5	Schedule downtime and make change	1 day	Tue 2/14/06	Tue 2/14/06	4	RR
6	**Improve high school LAN performance**	**27 days**	**Mon 1/23/06**	**Tue 2/28/06**		**PN,RR,KU,JT**
7	**Evaluate high performance servers**	**21 days**	**Mon 1/23/06**	**Mon 2/20/06**		**RR**
8	Establish test criteria	4 days	Mon 1/23/06	Thu 1/26/06		RR
9	**Establish pilot network**	**7 days**	**Mon 1/23/06**	**Tue 1/31/06**		**RR**
10	Obtain server	5 days	Mon 1/23/06	Fri 1/27/06		JT
11	Obtain typical clients	2 days	Mon 1/23/06	Tue 1/24/06		JT
12	Install NOS on server	1 day	Mon 1/30/06	Mon 1/30/06	10	JT
13	Configure NOS	1 day	Tue 1/31/06	Tue 1/31/06	12	PN
14	Install clients	1 day	Wed 1/25/06	Wed 1/25/06	11	JT
15	Test pilot network	14 days	Mon 1/30/06	Thu 2/16/06	10	KU
16	Summarize test conclusions	2 days	Fri 2/17/06	Mon 2/20/06	15	KU
17	Backup existing servers	2 days	Mon 1/23/06	Tue 1/24/06		PN
18	Document current configurations	2 days	Mon 1/23/06	Tue 1/24/06		PN
19	**Install high performance servers**	**4 days**	**Tue 2/21/06**	**Fri 2/24/06**	**7**	**PN,RR,KU**
20	Install NOS	2 days	Tue 2/21/06	Wed 2/22/06		PN
21	Restore data	1 day	Thu 2/23/06	Thu 2/23/06	20,17	PN
22	Restore configuration and object directories	1 day	Fri 2/24/06	Fri 2/24/06	21	PN,KU
23	Test installation	2 days	Mon 2/27/06	Tue 2/28/06	19	PN,RR,KU,JT
24	**Install WAN connection between high school and middle schools**	**6 days**	**Wed 2/15/06**	**Wed 2/22/06**	**1**	**JK,DL,RR,PN**
25	Purchase router	5 days	Wed 2/15/06	Tue 2/21/06		DL
26	Schedule downtime and make change	1 day	Wed 2/22/06	Wed 2/22/06	25	RR,PN
27	Install proxy server	2 days	Wed 2/15/06	Thu 2/16/06	1	

Figure 15-2: A project plan in Microsoft Project

Tasks and Timelines

- Project should be divided into specific tasks
  - Divide large tasks into sub-tasks
  - Assign duration, start date, finish date to each task and sub-task
  - Designate milestones, task priority, and how timeline might change
- Allow extra time for significant tasks
- Gantt chart: popular method for depicting when projects begin and end along a horizontal timeline

Tasks and Timelines (continued)

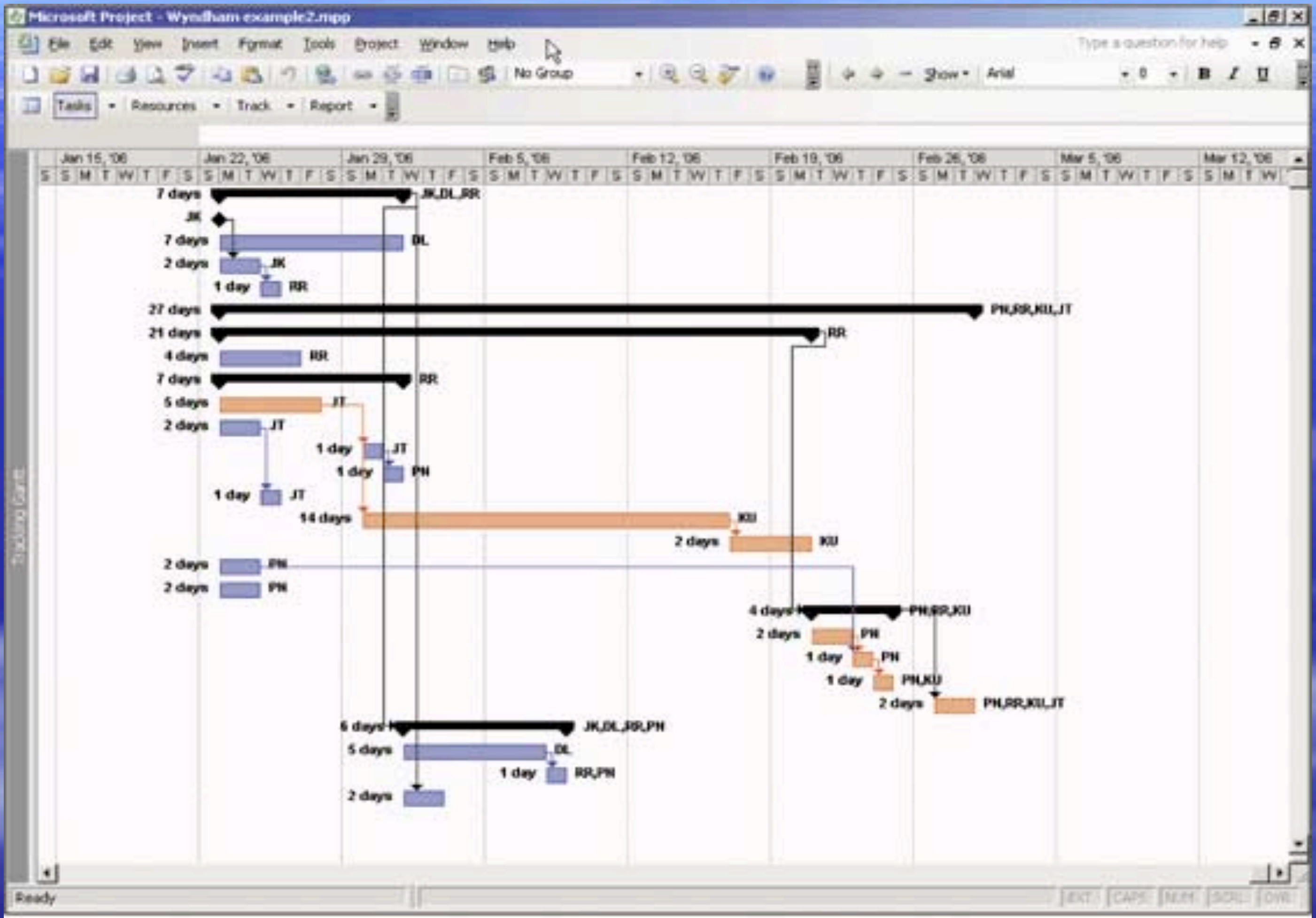


Figure 15-3: A simple Gantt chart

Communication

- Project manager responsible for facilitating regular, effective communication among project participants
  - Must communicate with stakeholders as well
- Must prepare users for changes:
  - How access to network will be affected
  - How data will be protected during change(s)
  - Whether you will provide means for users to access the network during change(s)
  - Whether users will have to learn new skills

Contingency Planning

- Even meticulously planned projects may be derailed by unforeseen circumstances
- Contingency planning: process of identifying steps that minimize risk of unforeseen events that could affect quality or timeliness of project’s goals

Using a Pilot Network

- Pilot network: small-scale network that stands in for a larger network
  - Used to test changes before applying to enterprise
  - Should be similar enough to closely mimic larger network’s hardware, software, connectivity, unique configurations, and load
- Tips for creating realistic and useful pilot network:
  - Include at least one of each type of device that might be affected by the change
  - Use same transmission methods and speeds as

Using a Pilot Network (continued)

- Tips for creating realistic and useful pilot network (continued):
  - Try to emulate number of segments, protocols, and addressing schemes in current network
  - Try to generate similar amount of traffic
  - Implement same server and client software and configurations as found in current network
  - Test for at least 2 weeks

Testing and Evaluation

- Test after completing each major step
- Must establish testing plan
  - Including relevant methods and criteria
- Testing should reveal:
  - Whether task was successful
  - Unintended consequences
  - Whether new needs exposed

Network Management

- In broad terms, assessment, monitoring, and maintenance of all aspects of a network
- Network management applications may be used on large networks
  - Continually check devices and connections to ensure they respond within expected performance threshold
  - May not be economically feasible on small network
- Several disciplines fall under heading of network management
  - All share goal of preventing costly downtime or

Obtaining Baseline Measurements

- Baseline: report of network's current state of operation
  - Baseline measurements allow comparison of future performance increases or decreases caused by network changes with past network performance
- The more data gathered while establishing the baseline, the more accurate predictions will be
- Several software applications can perform baselining

Obtaining Baseline Measurements (continued)

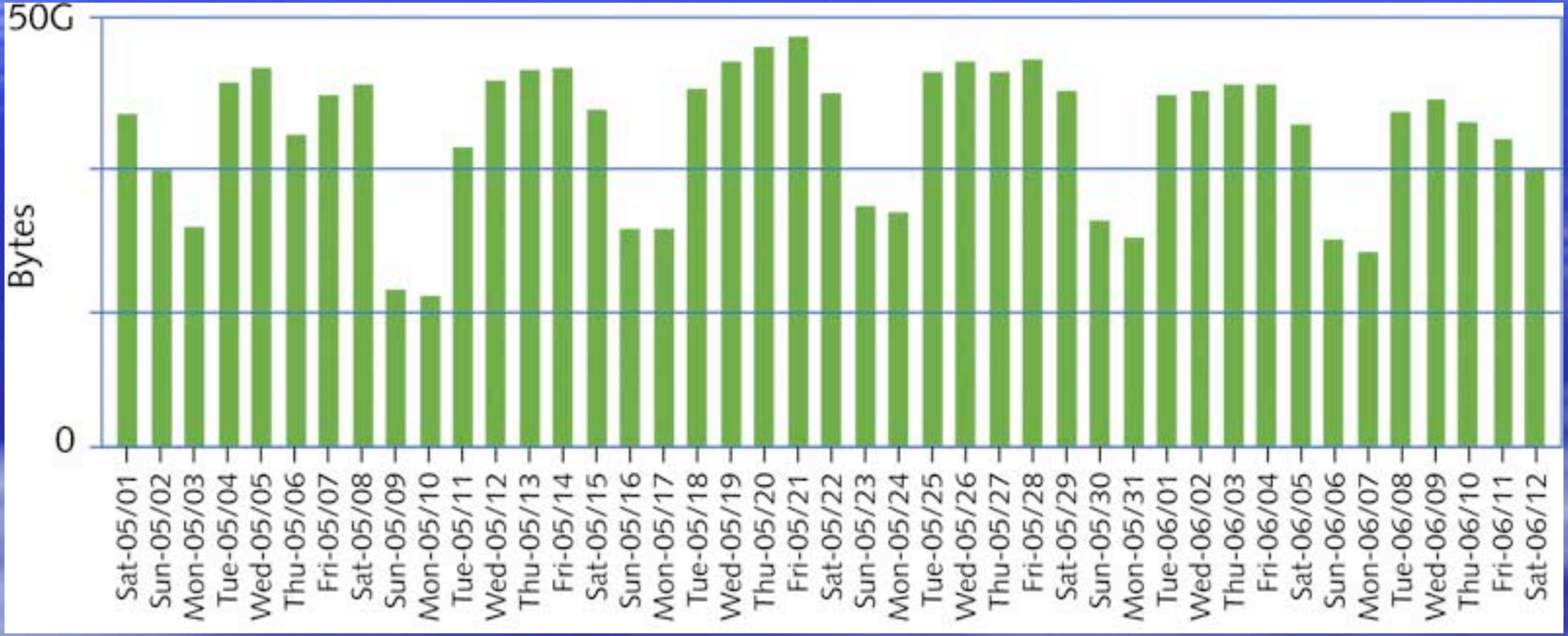


Figure 15-4: Baseline of daily network traffic

Obtaining Baseline Measurements (continued)

- Baseline assessment should address:
  - Physical topology
  - Access method
  - Protocols
  - Devices
  - OSs
  - Applications

Performance and Fault Management

- Performance management: monitoring how well links and devices are keeping up with demands
- Fault management: detection and signaling of device, link, or component faults
- Organizations often use enterprise-wide network management software
  - At least one network management console collects data from multiple networked devices at regular intervals

Performance and Fault Management (continued)

- Each managed device runs a network management agent
  - Collects information about device’s operation and provides it to network management application
- Definition of managed devices and data collected in a Management Information Base (MIB)
- Simple Network Management Protocol (SNMP): TCP/IP protocol used by agents to

Performance and Fault Management (continued)

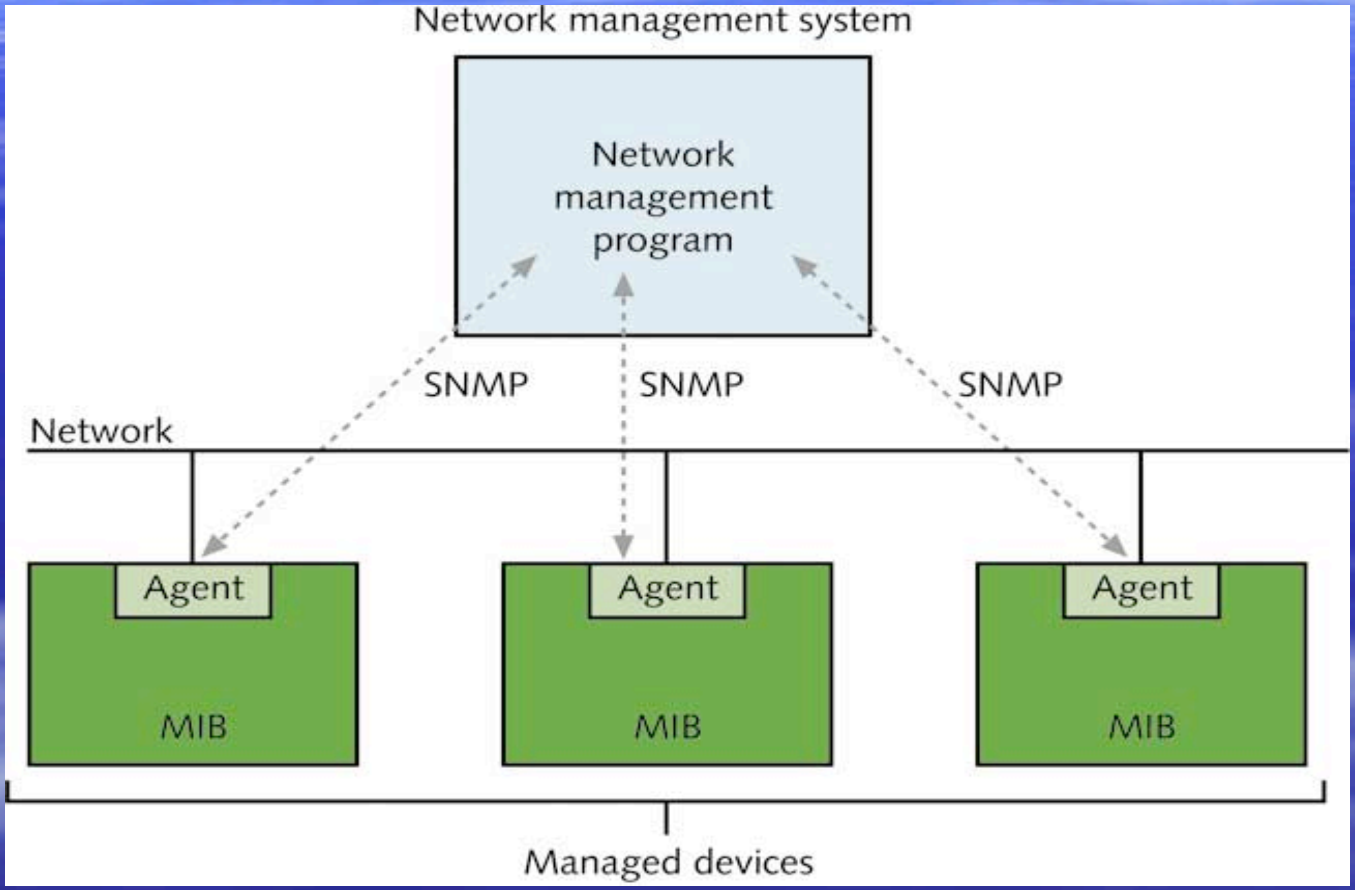


Figure 15-5: Network management architecture

Performance and Fault Management (continued)

- Network management application can present an administrator with several ways to view and analyze data
- Network management applications are challenging to configure and fine-tune
- Multi Router Traffic Grapher (MRTG): command-line utility that uses SNMP to poll devices, collects data in a log file, and generates HTML-based views of data

Performance and Fault Management (continued)

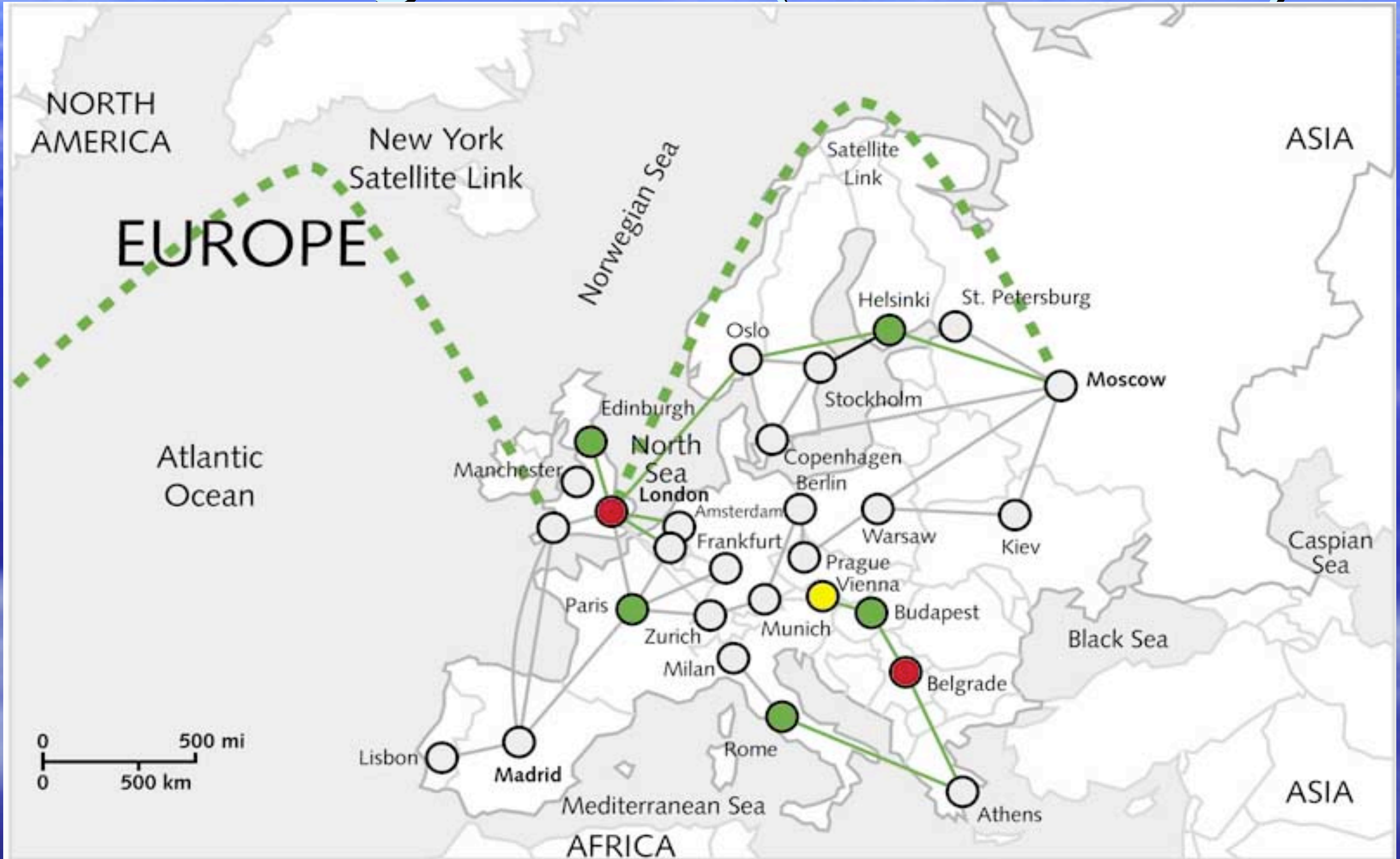


Figure 15-6: Map showing network status

Performance and Fault Management (continued)

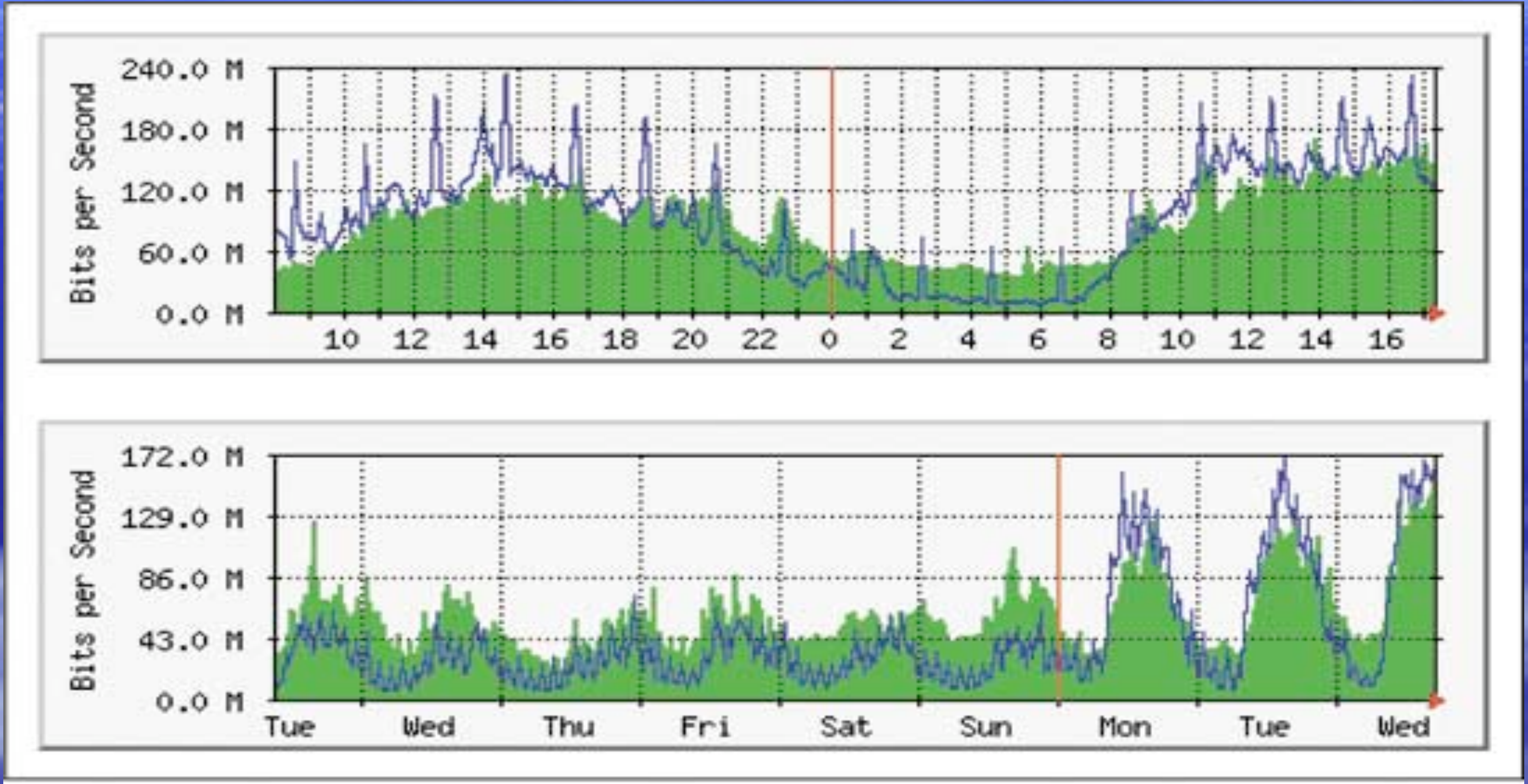


Figure 15-7: Graphs generated by MRTG

Asset Management

- Identifying and tracking hardware and software on a network
  - First step is taking detailed inventory of each node on network
- Asset management tool choice depends on organization’s needs
- Should ensure that asset management database regularly updated
- Simplifies maintaining and upgrading the network
- Provides info about costs and benefits of

Software Changes

- General steps:
  - Determine whether change is necessary
  - Research purpose of change and potential effects on other applications
  - Determine whether change should apply to some or all users
  - Notify system administrators, help desk personnel, and users
    - Schedule change for off-hours, if possible
  - Back up the current system or software

Software Changes (continued)

- General steps (continued):
  - Prevent users from accessing system or part of system being altered
  - Keep upgrade instructions handy and follow them
  - Make the change
  - Test the system fully
  - If successful, re-enable access to system
    - If not, roll back changes
  - Communicate changes made
  - Record changes in change management

Patches

- Patch: correction, improvement, or enhancement to particular piece of a software application
  - Changes only part of an application
  - Often distributed at no charge by software vendors
    - Fix bugs
    - Improve functionality
- Back up system before installing
- Install during off-hours

Client Upgrades

- Software upgrade: major change to a software package's existing code
  - Designed to add functionality and fix bugs in previous version of the client
- Typically overwrites some system files
  - Installation may affect other applications adversely
- Test on single workstation before distributing to all users
- Workstation-by-workstation or network

Shared Application Upgrades

- Apply to software shared by clients on network
  - Same principles as modification of client software
- Usually designed to enhance application’s functionality
  - Weigh time, cost, and effort against necessity
- For significant upgrade, may need to provide user training

Network Operating System Upgrades

- Usually involves significant changes to way servers and clients operate
  - Requires forethought, product research, and rigorous testing before implementation
    - May require specific project plan
- Consider the following in project plan:
  - Effect on user IDs, groups, rights, and policies
  - Effect on file, printer, and directory access
  - Effect on applications or client interactions
  - Effect on configuration files, protocols, and

Network Operating System Upgrades (continued)

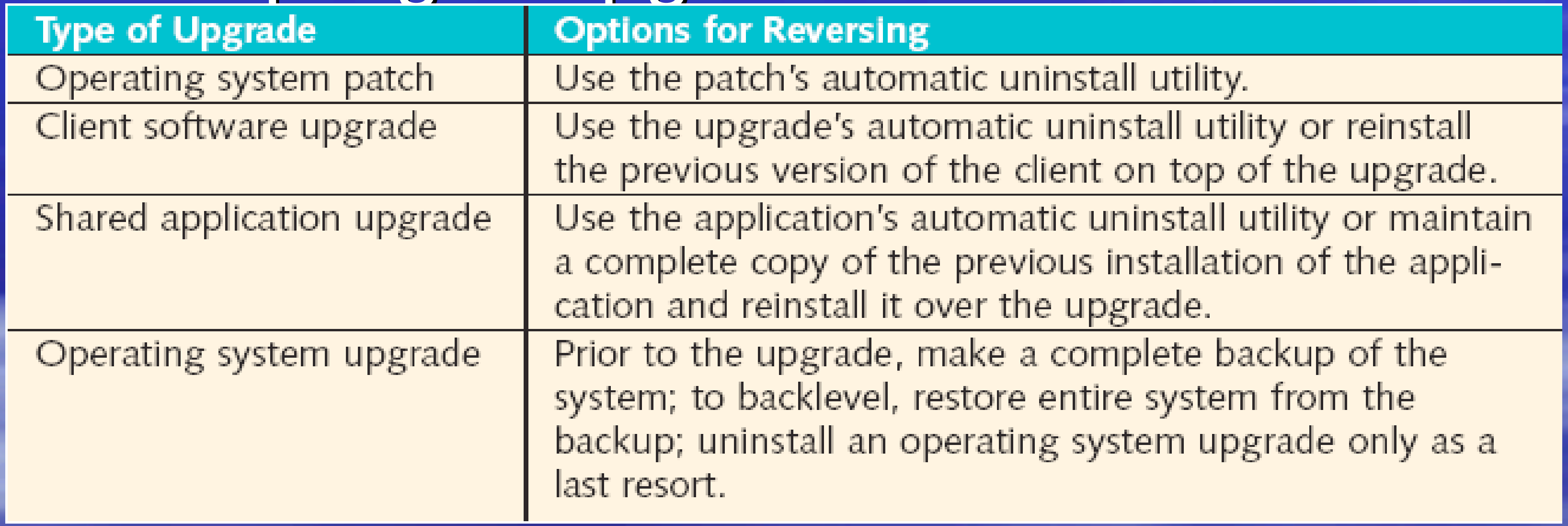
- Consider the following in project plan (continued):
  - Effect on server's interaction with other devices
  - Accuracy of testing in simulated environment
  - How it will be used to increase efficiency
  - Technical support arrangement with OS's manufacturer
  - Allotted enough time to perform upgrade
  - Can reverse the installation if troubles arise
  - Communicate benefits to others

Network Operating System Upgrades (continued)

- Basic steps for performing upgrade:
  - Research
  - Project plan
  - Proposal
  - Evaluation
  - Training
  - Pre-implementation
  - Implementation
  - Post-implementation

Reversing a Software Change

- Backleveling: process of reverting to previous version of software after attempting to upgrade



Type of Upgrade	Options for Reversing
Operating system patch	Use the patch's automatic uninstall utility.
Client software upgrade	Use the upgrade's automatic uninstall utility or reinstall the previous version of the client on top of the upgrade.
Shared application upgrade	Use the application's automatic uninstall utility or maintain a complete copy of the previous installation of the application and reinstall it over the upgrade.
Operating system upgrade	Prior to the upgrade, make a complete backup of the system; to backlevel, restore entire system from the backup; uninstall an operating system upgrade only as a last resort.

Table 15-1: Reversing a software upgrade

Hardware and Physical Plant Changes

- Often performed to increase capacity, improve performance, or add functionality to network
- Proper planning is key to successful upgrade
- Steps for changing network hardware:
  - Determine whether change necessary
  - Research upgrade's potential effects on other devices, functions, and users
  - Communicate change to others and schedule it

Hardware and Physical Plant Changes (continued)

- Steps for changing network hardware (continued):
  - – Keep installation instructions and hardware documentation handy
  - – Implement change
  - – Test hardware
    - Preferably with higher than normal load
  - – If successful, re-enable access to device
    - If not, isolate device or reinsert old device
  - – Communicate results of changes to others
  - – Record change in change management system

Adding or Upgrading Equipment

- Difficulty depends largely on experience with specific hardware
- Networked workstation: simplest device to add
  - Directly affects only a few users
  - Does not alter network access for others
- Networked printer: slightly harder than adding networked workstation
  - Shared, unique configuration process
  - Time required to install does not usually affect

Adding or Upgrading Equipment (continued)

- Hub or access point:
  - Only worry about downtime if upgrading or swapping out existing hub or access point
  - Must consider traffic and addressing implications
- Server requires great deal of foresight and planning
  - Consider hardware and connectivity implications, as well as issues relating to NOS
  - Add while network traffic low or nonexistent
  - Restrict access to new servers

Adding or Upgrading Equipment (continued)

- Switches and routers: often physically disruptive
  - Affects many users
  - Router or switch may have unintended effects on segments other than the one it services
  - Plan at least weeks in advance
  - Keep safety in mind
  - Follow manufacturer's temperature, ventilation, antistatic, and moisture guidelines

Cabling Upgrades

- May require significant planning and time to implement
- Best way to ensure future upgrades go smoothly is careful documentation of existing cable
- Upgrade cabling in phases
- Weigh importance of upgrade against potential for disruption
- Larger organizations rely on contractors who specialize in cabling upgrades

Backbone Upgrades

- Most comprehensive and complex network upgrade
  - Upgrading entire backbone changes whole network
- Examples:
  - Migrating from Token Ring to Ethernet
  - Migrating from slower technology to faster one
  - Replacing routers with switches
- May require upgrading cabling and hardware
- First step is to justify upgrade

Reversing Hardware Changes

- Provide a way to reverse hardware upgrades and reinstall old hardware if necessary
  - Keep old components safe and nearby
- Old hardware may contain important configuration information

THANK YOU

QUESTIONS?