

"People who deal with bits should expect to get bitten."
- Jon Bentley



Topics

Scanning

The Complete PC Network

Hands On

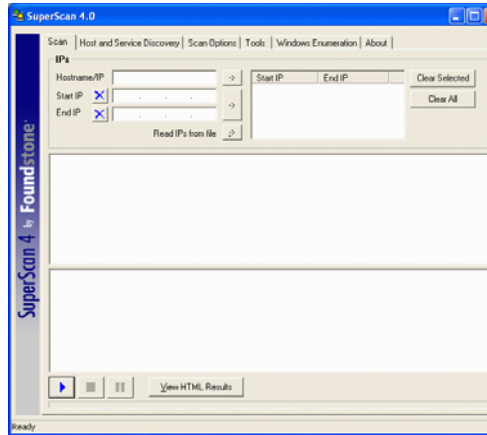
Port Scanning

Port Scanner

BE VERY CAREFUL - CAN BE PERCEIVED AS AN ATTACK!

Download SuperScan from Foundstone

Port Scanner



Scans

Scan your machine (127.0.0.1)
Scan
192.168.0.22 Windows 98
192.168.0.23 Windows 2000
192.168.0.24 Linux
192.168.0.25 Mac
Scan All Machines 192.168.0.1-255
Windows Enumeration
Enumerate some systems
Turn firewall on - rescan
Does it make a difference?

Scans

So what did we find out?

Network+

The Complete PC Network

Complete PC Network

Connections to the network
Speed
Reliability
Protection of Data
Specialized hardware

Connecting to a Network

Network Interface Cards

Connectors

Cabling

These determine the speed and capabilities for this node

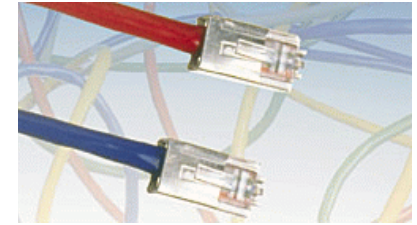
The Connectors

BNC
British Naval Connectors
Bayonet Neil-Concelman



The Connectors

RJ Connectors
RJ-11 Telephone
RJ-45 Networking



The Connectors

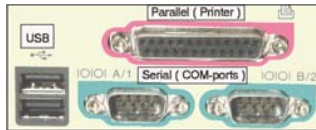
DB Connectors - D Shaped

DB-25 RS232

DB-9 RS232

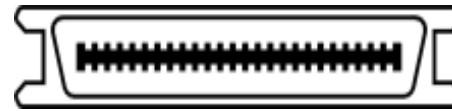
DB-15 VGA Video

Male vs. Female



The Connectors

Centronics
36 pin Printers
50 pin SCSI



The Connectors Fiber Optic



SC

ST



FDDI

Fiber Distributed Data Interface

The NICs

Connects PC to network

Connectors

Speed

Duplex

Must match the network

Ethernet NICs

10Base5 - Thicknet
15 pin DB connector DIX
Connects to AUI
Attachment Unit Interface

10Base2 - Thinnet
BNC connector

Ethernet NICs

10BaseT
RJ-45 Connector

100BaseTX, 100BaseT4
100BaseVGAnyLAN
RJ-45 Connectors

10BasedFL, 100BaseFX
Fiber Connectors

Token Ring NICs

DB-9

RJ-45

How to tell the difference between cards?

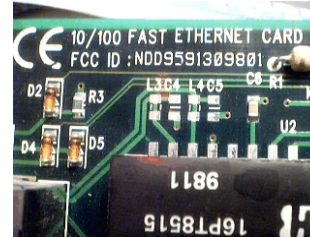
FCC ID Search Engine

FCC ID

Almost every device has one.

Can be used to identify a manufacturer of a generic component.

Who made this?



The Modems

Internal Modem
1 or 2 RJ-11 Connectors

External Modem
RS-232 Cable, 9 or 25 pin

Baud vs. BPS

Baud - Signals per second

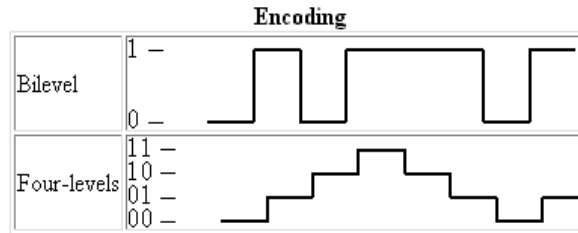
BPS - Bits per second

Can be the same, or different

BPS = Baud * Bits per Signal

9600 = 2400 * 4

Baud vs. BPS



Same Baud, twice the BPS

System Resources

Most system are plug and play

Some are not

Different devices need
IRQ
DMA
Port Number
Memory

IRQ

Interrupts

Allows system to multitask

Only one device can use an IRQ

Common IRQs

IRQ	Use
3	Serial Port
4	Serial Port
5	Secondary Parallel Port
7	Primary Parallel Port
10	Typically Available
11	Typically Available
12	Typically Available

Varies from System to System!

DMA

Direct Memory Access

Fast Data Transfers

Common DMA Channels Available
1, 3, 5, 6, 7

Memory

Some NIC cards require some reserved memory for proper operation

Video Cards also reserve memory

Ports

Input / Output Address

Port	I/O Address	IRQ
COM1	03f8	4
COM2	02f8	3
COM3	03e8	4
COM4	02e8	3
LPT1	0378	7
LPT2	0278	5

Checking System Resources

Control Panel -> System

Device Manager
Computer
Properties

Select Devices
Check the Resources

Installing Modems and NICs

Physical Connections

Bus Type

ISA 8 / 16 bit

PCI

Jumpers / Switches

Only on older ISA cards

Before Installing

Turn off / Unplug Computer

Ground yourself

Can damage components with static electricity!

Installing

Drivers

Assigning Resources

Diagnostics

Buying Cards

Stick with big names

Linksys, Intel

Check website for drivers

Find a common type

Fewer drivers

Direct Cable Connections

Not used much anymore

Serial- Serial

Null Modem Cable

Parallel-Parallel

Much faster

Special Cable - Laplink

Protection of Data

BACKUPS

Redundant component technology

RAID

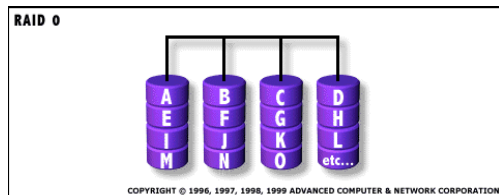
Random Array of Inexpensive Devices

Random Array of Independent Devices

Fault tolerant systems - RAID

Win NT supports RAID 0,1 and 5

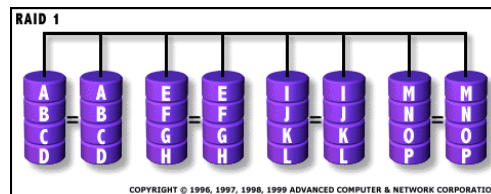
RAID 0 - disk striping - disk striping divides data into 64k block and spreads it equally among disks



Fault tolerant systems - RAID

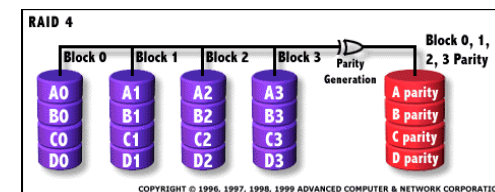
RAID 1

disk mirroring - duplicates a partition on another disk
duplexing - mirrored pair of disks with an addition disk controller



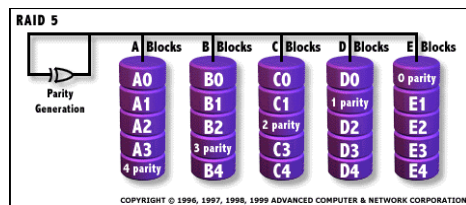
Fault tolerant systems - RAID

RAID 4 - disk striping with parity data is striped to multiple drives and then its parity sum is calculated, which is written to the dedicated parity drive



Fault tolerant systems - RAID

RAID 5 - striping with parity - data is striped across multiple drives and then its parity sum is calculated, which is also striped across multiple drives.



Fault tolerant systems

Sector spacing - SCSI - hot fixing automatically moves data from bad to good sectors

How Swapping
Removing / Replacing a drive with the system turned on.

Drive Technology

EIDE
Enhanced Intelligent Device
Electronics

PC typically can have 4 EIDE devices

Drive Technology

SCSI
Small Computer System Interface

Host Adapter

Devices are connective via a chain

SCSI ids
0 -7 (7 is the host adapter)

RAID Implementation

Windows / UNIX support RAID

Hardware/Software Implementation

Disk Administrator

Tape Backup

Many different Kinds
QIC - Quarter Inch Tape
40mb - 8gb
DAT - Digital Audio Tape
Up to 24 gb
DLT - Digital Linear Tape
Up to 70 gb

Data Redundancy Is the Key

BACKUP

BACKUP

BACKUP

Multiple Copies

Multiple Locations

Speed

It is never fast enough

People get used to the faster speeds

Use expands to fill capacity

Fast NICs

Increase Megabits
10 - 1000 Mbps

Full Duplex

Smarter NICs
On board processing

Faster!

Make the Drives Faster
EIDE, SCSI, RAID

More RAM

Upgrade the Hubs

Use switches instead of hubs

It's Not Just Hardware

Network Design

Bottle necks

Driver configuration

Reliability

How reliable is your system?

Weakest Link is the chain sets the pace,
lowers everybody

Sysrel.exe

In Class

If an ATM is 98% reliable and the telcom
line it uses is 95%, and the computer it
accesses is 99%, what is the total
system reliability?

Downtime

How often is you system available?

How does reliability affect downtime?

Downtime.exe

In Class

If an ATM is 98% reliable and the telcom
line it uses is 95%, and the computer it
accesses is 99%, what is the total
system reliability?

What would be the total downtime in
minutes for a 24 hour day?

<p>Interesting Fact</p> <p>Reliability of US Phone System</p> <p>Failure rate of entire central office is once in 40 years.</p> <p>If down 1 day in 40 years overall reliability = 99.993155% Component reliability?</p>	<p>"The 5 Nines"</p> <p>In the IT industry, server operating system reliability is expressed in terms of "nines."</p> <p>99.999% is referred to as "five nines." Regarded as the highest number realistically achievable, 99.999% is less than five minutes downtime per year.</p>	<p>MTBF and MTTR</p> <p>Mean Time Between Failures How often can we expect failures?</p> <p>Mean Time to Repair How long will it take to repair?</p> <p>MTTP...</p>
<p>Reliability</p> <p>Without power, system is worthless</p> <p>Power Problems Spikes Sags</p> <p>Big Issue: California Power Outages Sun losses 1+ million per minute</p>	<p>Good Power</p> <p>Dedicated Circuits</p> <p>Surge Suppressors</p> <p>UPS Uninterruptible Power Supplies</p> <p>Backup</p>	<p>Environment</p> <p>Keep server room locked</p> <p>Control Access</p> <p>Control Temperature / Humidity 60 degrees, 40% humidity</p>
<p>Redundant Components</p> <p>Have spares on hand</p> <p>Have pre-loaded hard drives</p> <p>Stand by units</p> <p>Practice swapping them</p>	<p>How Much Reliability Do You Need?</p> <p>More reliability Most Cost</p> <p>What is your MTTP? Mean Time To Pain</p> <p>IBM Commercial</p>	<p>End of Lesson</p>