The Dynamic and Depreciating Value of Computers

Summary: an attempt at evaluating computers based on configuration and activity. The value changes over time in a modest attempt to deal with real-word changes in valuation.

Irrespective if we actually could come up with a reasonable method, the thought of knowing how much money was tied up into our systems and how much effort or damage we'd incur when problems befell is compelling. I believe that we can come up with an automatic and consistent method of quantifying the value of things that, while not claiming to be stunningly accurate, has an opportunity to give at least an interesting evaluation of a network, and one that I suspect won't be so wildly off that it would prove to be useless. Even that might not be too interesting – esp. if our estimates were really off – but when married with compliance and policy, and emphasizing the *rate of change* over time… that starts to sound good. And if we add in the thought that we could automatically depreciate things, so that more contemporary data and hardware has more value, things might be even better.

Here are some of the basic things of value that we can use to estimate the value of computers:

- Hardware & Software
- Document types and numbers present on a system
- Activity

In addition users might have three bits of information that could be manually entered by someone who understands the organization or specific systems that would influence the calculations:

- Overall organizational (network/computer) worth
- Estimated total hosts on the network
- The dollar value of an individual system

I'll talk about each in turn, along with some implementation notes. But the basic premise is that for each computer you add up each area and come up with a dollar amount for that host. This is not exactly a replacement value, but instead some estimate of how much that host is worth if it were compromised or if (something like) the worst happened.

The total value of an organization is simply all the individual values added up.

You could use "credits" instead of "dollars" or even remove the label altogether, of course.

Organizational Value

I. Overall network/computer worth

An admin user also has the option (in the configuration section or some other area) to assert that their entire network is worth X dollars. The calculations are then performed for all individual systems as per usual, but the individual values are adjusted as follows:

> Assume the overall value of the network is valued at N dollars by the user; the adjusted value is multiplied by:
>
> (X/ (X % N))

For instance, if the network was estimated to be worth $100M by the user and you found a total value of $50M, you would multiply the value of individual systems by:

> 100M * (100M % 50M) = 2

Obviously this could elevate or diminish the value of the network or individual hosts.

II. Estimated hosts on the network

If we don't have good penetration into the organization's network, values seen are less accurate and should be adjusted. The admin user may optionally enter (in the configuration section or some other area) how many hosts they think they have; if we have seen fewer hosts than that we multiply the aggregate network worth by the ratio of what we have seen vs. what they claim. For instance, if they say there are 10K hosts and we have only seen 5K, multiply the calculated worth of the network by .5.

This is (not-very ;-)) analogous to the dark matter in the universe and the calculations of mass; it's out there somewhere, we just don't know where.

This calculation is done after any "overall network/computer worth" adjustments are performed.

Individual Host Values

I. The dollar value of an individual system

For certain key systems no automated analysis would be sufficient to calculate a reasonable value. For instance a source code repository that held all of a company's intellectual property might be valued at ten million dollars or more.

A user should be able to go to a host and manually enter in a dollar figure for the additional worth of a system above and beyond what is calculated. This number will simply be added to the calculated value for that system in question (a negative value will cause the value of the system to drop, but not below zero value.)

The estimated dollar amount should not be changed by organizational multipliers – it is an unadulterated estimate of the computer's value, and this shouldn't be influenced by our calculations.

II. Hardware & Software

There are two methods that can be used – the EZ and the long forms. The EZ method should be OK for the first implementation of this report, while the long form is a work in progress and was started in an earlier version of this document.

EZ form

Hosts get a value assigned to them based on some gross characteristics; these are either calculated from group membership or from host attributes:

Agents – AIX	$20000
Agents – HP	$10000
Agents – Mac OS X	$5000
Agents – Sun Solaris	$10000
Agents – Windows 2000	$8000
Agents – Windows 2003	$10000
Agents – Windows XP	$5000
Agents – Red Hat Linux	$7500
Other/unknown	$3000

There are modifiers as well; if a system falls into one of these categories add this cost.

Enterprise Agent	+100% of base cost
Laptop	+$1000
Multiple CPUs	Each CPU adds %50 of the base cost

There are other types of groups that effect the cost, but they will be factored in other sections.

Hosts that do not run the agent should take a different approach to this calculation. If the OS or hardware type is known than the price (in this section) for an average agent with the same OS or hardware type should be used. If even this isn't know about a host than the average overall cost for an agent should be used.

III. Documents

[This section only impacts agents running Windows. It might be expanded in later versions.]

I'm guessing that the more starched of the white collars probably have more .DOC, .XLS, and .PPT files than others; perhaps the higher up you go (up to a point) the more you see? These documents often contain IP or company secrets you don't want others to see. Here's another SWAG for each unique document that you find on an individual's computer (ONLY in their personal area) the enterprise[1]:

Document type	Value per document
.PPT	$1000
.DOC	$1500
.XLS	$2500
.FM (FrameMaker document)	$5000
.DWG, .DWF (AutoCad)	$5000

I'd do a position-in-the-organization multiplier (are a CEO's docs worth more than an engineers, I wonder? ;-)), but that's pretty much impossible to get without outside input. And I'm trying to get some real #'s to see how many docs people like the CEO, VP of marketing, and other types create and have. Not sure how to do this for programmers (how much is a line of code worth, where is it, etc.), but I'm thinking about it.

Documents generally are less valuable as time goes on, Shakespeare notwithstanding. I assign a half-life of 90 days to a document, which means that after it was created or the last modification that it halves in value every 90 days. So that MS word document that is a year old (roughly 360 days, or four halvings of value) is worth 1500/(2*2*2*2) = $187.50.

To calculate these values a new policy will have to be written that sums up these values for an agent and return this to the server.

Hosts that do not run the agent should take a different approach to this calculation. If the OS or hardware type is known than the price (in this section) for an average agent with the same OS or hardware type should be used. If even this isn't know about a host than the average overall cost for an agent should be used.

IV. Activity

Enough about the hypothetical, let's talk about the real… well, the virtual real, at least. Here we'll talk about the activity levels of computers – for now we can use the last day of measurements.

[1] http://www.ace.net.nz/tech/TechFileFormat.html has a billion different extensions, if we want more.

Machines that get requests and send information out in response to others can be generally thought of as an interesting class of hosts. And the more activity and more systems they talk to the more important they are, for a variety of reasons. Let's try to quantify this.

I've split the type of activity into three types – total number of inbound sessions, number of bytes sent out, and the number of different hosts talking to the system. To get the activity value you add up all three values (cumulative values follow the Fibonacci pattern – hey, if it's good enough for seashells and sunflowers, it's good enough for us!):

Total inbound connections:

# of sessions	**Value per connections ($)**	
1-20,000	0.50	
20,001-100K	0.125	$10K + this value
100,001-500K	0.025	$20K
500,001-2M	0.0067	$30K
2M+1 – 10M	0.002	$50K
10M+1 – 100M	0.0003	$80K
100M+	0.00005	$130K

Total bytes/day outbound:

# bytes	**$ per K/bytes**	**Cumulative value**
10MB-40MB	0.25	
40-100MB	0.1667	$10K + this value
100MB - 691.2 MB (64 Kbs)	0.0169	$20K
< 2.7648 GB (256 Kbs)	0.0067	$30K
< 16.675 GB (1.544 Mbs – T1))	0.0014	$50K
< 108 GB (10Mbs)	0.0003	$80K
< 1.08 TB + (100Mbs)	0.00005	$130K

Unique [prefer only inbound] hosts communicating:

# hosts	**$ per host**	**Cumulative value**
1-1000	0.10	
1001-2500	0.04	$10K + this value
2501-10,000	0.01	$20K
10,001-50,000	0.002	$30K
50,001-250,000	0.0004	$50K
250,001-1,000,000	0.00001	$80K
> 1,000,000	0.000001	$130K

In addition certain types of servers suggest the host is more valuable than the mere traffic patterns. A bit more of the back of the envelope some value propositions (simply multiply the numbers above by this), along with some guesses as to how relevant the above numbers would be to the specific type of server listed; these are looked up based on the group of the system in question:

Group	**Multiplier**	**Raw #**	**Traffic Volume**	**Unique hosts**
Hosts - Name Server (e.g. DNS, Active Directory, NIS)	1.5 (pretty darn important)	High	Low	High
Hosts – Web Server	1.0	High	High	Med
Hosts – Secure Web Server	2.0	Low	Med	High
Hosts – Mail Server	1.3 (moderately high volume, but really important)	Med	Med	Med
Hosts - DB (port 1521/oracle, 523/DB2, 5432/postgres + mysql)	2.0 (perhaps the most valuable kind?)	Low	Med	Low
Hosts – DHCP	1.5 (low volume, high value)	Low	Low	Low
Hosts – File Servers	1.2	High	Med	Low
Other (no above groups)	1.0 (as listed)	???	???	???

I suppose you can simply multiply them if they're the same box – if someone is foolish enough to put their web, mail, SQL, etc. on the same machine – since if they do that the traffic shouldn't be too high so the valuation will all come out OK.

So, for example, a corporate mail server that delivers 50K documents a day, each mail message averaging about 5K per doc to 1000 recipients would be worth $60170.5 ($13,750 (connections) + 22,535 (traffic) + 10,000 (unique hosts) * 1.3 (mail server multiplier.)) That doesn't seem ridiculous; the highest volume servers might be worth some hundreds of thousands of dollars, which, if anything, is an underestimate.

Hosts that do not run the agent should take a different approach to this calculation. It's safe to assume that there is a good chance that we don't have complete traffic stats for the system in question. In order to compensate for this we apply a multiplier. This is determined by:

$$(1-X) * 10 + 1$$

Where X is a percentage; either divide the “estimated hosts on the network” or the number of inside hosts observed (whichever is greater) by the number of agents inside an organization.

This will give you a multiplier from 1-11 (if you have 100% penetration the system in question will be running an agent as well, so you ignore this calculation, but it approaches this.)

III. Total Value

Add up the individual systems, applying any host or network modifications, and that’s the estimated value of the network. The individual host raw and adjusted dollar values are displayed in the SHV along with any modifiers, if applicable. The overall network value is in a separate report, along with the adjustments and final adjusted #, with the hosts and how much they contribute in a one-per-line as-per-usual report; the standard host line with one additional number, that being the adjusted $$$ of the system in question.

There should be an adjusted $$$ over time graph for both the individual host and the organization.

IV. Implementation Note

Obviously this isn’t an exact science. Major Hint - it would be extraordinarily useful to have all the tables and calculations in a configuration file that could be modified by an SE, so adjustments/tweaks could be made to better reflect reality as we move forward. E.g. if you don’t do this by a data/conf/table-driven approach you’ll be sorry.