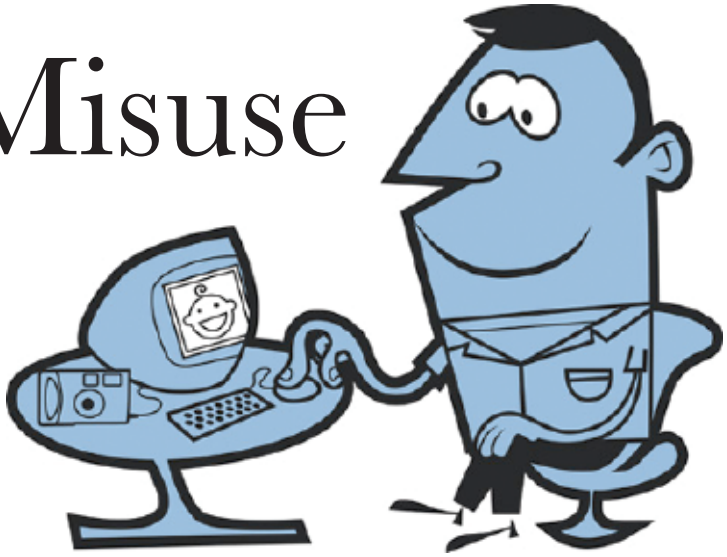
Identifying Network Misuse



Jim Metzler
Ashton, Metzler & Associates

I recently participated on two seminar tours hosted by Network World. The first tour was on the topic of Network Management, and the second tour was on the topic of WAN optimization. In each of the eight cities that these tours went to, the feedback from the audience was clear on a very important topic. That topic being that very few IT organizations have a detailed level of visibility into what traffic is running over their IT infrastructure.

That lack of visibility impacts IT organizations in a variety of ways. For example, as was discussed in depth on the seminar tours, this lack of visibility makes it virtually impossible for an IT organization to effectively manage application performance and ensure that key applications such as SAP or VoIP are performing adequately.

However, there is another significant negative impact that results from this lack of visibility. IT organizations that do not have visibility into the traffic that runs over their infrastructure will not be able to identify and control network misuse. For the sake of this IT Impact Brief, network misuse will be defined as those instances in which a portion of the company's network is being consumed by supporting traffic that is unauthorized and inappropriate.

Controlling network misuse can be thought of as a bandwidth optimization technique similar to compression and caching. In particular, if companies can control network misuse, it typically frees up a lot of additional bandwidth for legitimate traffic. While controlling network misuse has always been important, it is currently growing in importance due to all of the creative and taxing forms of misuse.

I first became aware of network misuse well over a decade ago when I was living in Boston and was involved with running the network for Digital Equipment Corporation (DEC). At the time, DEC was beginning to struggle in the marketplace and every one of DEC's support organizations, including IT, was under intense pressure to cut costs by 20%.

While the DEC IT organization was under this intense pressure to cut costs, we became aware of the fact that one of DEC's engineers had taken upon himself to download weather maps multiple times an hour onto his workstation. To make matters worse, the engineer made the entire engineering organization aware of what he was doing and many of them would regularly download weather maps off of his workstation and onto theirs. Since DEC did engineering on a worldwide basis, these downloads put a lot of extra traffic on DEC's LAN and WAN infrastructure.

It is worth noting that our efforts to eliminate this traffic were rebuffed by DEC's engineering organization. There rationale was that DEC's struggles in the marketplace made it difficult for them to attract and retain engineering talent. They strongly objected to the IT organization doing anything that would further erode the morale of the organization.

A few years later, I was consulting for a large company in the agriculture industry that was very interested in controlling the cost of their WAN. I suggested to them that one technique that they could use to control WAN costs was to make sure that they kept inappropriate traffic off their WAN. To exemplify this point, I told them about the story about the weather maps. The company was very interested in controlling network misuse, but pointed out that in their company having timely access to weather maps was a key requirement for their commodity traders.

This story raises a number of key questions that IT organizations should answer relative to network misuse:

1. Is there a policy that defines acceptable use of your company's IT resources?
2. Is there a program in place to educate your company's employees on this policy?
3. Are you aware of what traffic is transiting your IT infrastructure?
4. Is it possible to determine whether or not this traffic is appropriate from a business perspective?
5. Do you have the ability, from both a technical and political perspective, to identify the users and control any misuse?

Another situation that exemplifies the importance of the preceding questions concerns an insurance company that discovered streaming video consuming bandwidth in one of the company's branch offices. Further investigation revealed that an employee was logged into the web site of his child's daycare and was viewing their child's behavior view a web camera during the workday. Certainly if many employees of this company had followed the lead of this employee the network would be swamped with traffic.

On the surface, this sounds like a clear case of network misuse, and one that could have a very negative effect on the company's network. However, if the company were actively promoting itself as the employer of choice for working parents, removing this traffic would not only violate that promotion, but could also violate the company's human resources policies.

Most situations of network abuse are more clear-cut than the parent installing the nanny-cam. For example, virtually all companies agree that spam, Spyware and Adware have no legitimate business purpose and are attempting to control them. The same can be said about employees playing doom or sharing music files. Below is a list of other real life examples of network abuse.

- *A credit union discovered that one of their branch office employees was consuming half the branch's FT1 by listening to Internet radio.*
- *This abuse is not isolated. Another company discovered that a number of their employees listened to Internet radio – so many that Internet radio was their top application.*
- *A global telecommunications company determined that 83% of the utilization of one of their Packet over Sonet (POS) links was consumed with Peer-to-Peer applications.*
- *One company found a server had been taken over and was hosting movies.*
- *Another company found that one of their FTP servers was being externally controlled for the purpose of hosting and sharing games.*
- *One company discovered that one of their employees was a big Jimmy Buffet fan – so much so the user was continually streaming music from a Jimmy Buffet web site.*

As I mentioned at the top of this brief, I used to live in Boston. Like virtually all Bostonians, I am an avid (a.k.a., fanatical) Red Sox fan. Now that I live in Florida, I don't get to Fenway Park very often. Thankfully, I can watch Red Sox games on my PC by accessing MLB.com*. To me that is not network misuse – but using my network for a truly noble purpose. Of course, your managers might not agree.

*http://mlb.mlb.com/NASApp/mlb/mlb/video/mlb_tv.jsp?partnerId=180x150_mlbtv_bos