

Re: To vlan or not to vlan, that's the question

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2005-03/1196.html>

From: Xous – Jose R. Negreira (xous_at_xouslab.com)

Date: 03/31/05

Date: Thu, 31 Mar 2005 12:22:08 -0300

prg, thanks for your kind and long answer.

I **really** appreciated it, and just with a few words, I've learned a lot!!

What you suspect were the same as mine. Now I completely realize that I don't need VLANS.

"They (vlans) will not inherently add to your security and performance that you could not achieve with conventional switching/routing."

So, a conventional switching–routing solution will be a better cost/benefit solution (and about cost i'm talking about money, and configuration administration), due to the current network size and structure, no VoIP plans, etc. The real life example network (3000 nodes, 30 campus), are really outstanding numbers, we're talking definitively about different stuff. Thanks 4 showing me the way!

Regards,

--

Jose R. "Xous" Negreira

[*xous*at*xouslab_dot_com*]

XousLAB - <http://www.xouslab.com>

iptableslinux - <http://www.iptableslinux.com>

prg escribió:

> Xous - Jose R. Negreira wrote:

>

>>Hello everyone, 1st. post on this group here! (hope it's the right

>

> place)

>

>>Actually the network I administer, consists of actually 3 networks,

>>INTERNAL, DMZ, and EXTERNAL, that may be a familiar scenario for most

>

> of

>

>>you, simple and effective. The three networks, are interconnected

>

> with a

>

>>firewall (on a linux box, using netfilter). I was asked to literally

>>divide the network in two (phisically and/or logically), intending to

>

>

Re: To vlan or not to vlan, that's the question

comp.os.linux.networking: Re: To vlan or not to vlan, that's the question

```
>>improve security & performance.
>>
>>That's why we considered the option of a switch with VLAN support
>
> (but
>
>>we haven't done it in a serious way yet). Notice that we're talking
>>about a network with <100 hosts, counting servers and workstations.
>>
>>The 1st. question is:
>>1) Why would I spend $$ on a switch that supports VLAN, among other
>>features(*), if (IMHO) I can implement the same thing with 2 common
>>switches (less money), and a firewall interconnecting them (managing
>>security & routing) ?
>
>
> Unless you will now or in the near future implement vlans there is no
> real reason to spend more $ to get more (unused) features. But many
> newer, high speed switches are vlan capable anyway -- little $
> difference.
>
>
>>beside the -probable- answer is 'you just don't need vlan!!! Don't
>
> burn
>
>>money!', please let me write some additional questions:
>>
>>2) in what environment is really worthy implement vlan?
>>Google took me here:
>>http://nislalab.bu.edu/nislalab/education/sc441/six/implementation.htm
>>"Why implement Vlan?" but, It'd be nice to see comments about some
>>real-life examples.
>
>
> VLANs allow you to design/assign nodes by functional commonality
> without depending on _physical_ location. You will still require
> routers to route traffic _between_ different vlans as well as switches
> that support vlan trunking (to transport multiple vlan traffic across a
> common link). Thus print and file servers may be more "easily"
> positioned. This has given rise to greater centralized administration
> and server farms in the school district. The district has more than
> 3000 nodes scattered across more than 30 campuses. Thus geography
> within and between campuses and the NOS servers are more easily
> "conquered". The logical network is more "logical";)
>
>
>>3) What can I do with a vlan switch than I CANNOT DO with 2 switches?
>
>
> Create vlans ;) It may be easier to control traffic/bandwidth to
> accommodate varied requirements of nodes. Thus office/admin nodes are
> easier to accommodate _and_ isolate from student accessible nodes.
> Allows library nodes to incorporate outlying stations. Still debating
> whether to interconnect the high school libraries on a common vlan.
> For me the greatest vlan advantage is the way you can overcome
> geographical/physical location.
>
>
>>4) The firewall/router interconnecting both networks will have any
>>special issues to consider if the interconnected networks are a vlan
>>network, or are independent?
```

comp.os.linux.networking: Re: To vlan or not to vlan, that's the question

```
>
>
> Not generally if you design the vlans and IP network(s) properly.
>
>
>>(*) there may be other features, that I don't know, and even I may
>
> not
>
>>need, but this can be gently answered in question 2 ;)
>
>
> Unless you have a pressing need for vlans there is no reason to go that
> route, IMHO. They will not inherently add to your security and
> performance that you could not achieve with conventional
> switching/routing.
>
> If your physical distribution of nodes makes managing network
> resources/access difficult, then I would seriously consider vlans as a
> possible solution.
>
> If you require more centralized control/administration of network
> resources, then again I might consider vlan switching.
>
> The "flexibility" and "ease of management" offered by vlans require
> proper up-front setup (eg., MAC tracking) and may require "management
> software" to keep a handle on everything.
>
> For a given amount of $ you may be able to get better throughput
> speeds/latencies with conventional switches and good GigE (fiber)
> links.
>
> With only 100 nodes, I suspect that you don't really need vlans as
> opposed to conventional switching. In fact, vlans are usually combined
> with conventional switching. Could you substantially reduce the
> number/use of routers by implementing a switched vlan network?
>
> Much of the flexibility of vlans can be implemented with good use of
> DHCP and policy routing. At some point vlans are "easier" for carving
> up networks according to differing resource/bandwidth requirements, but
> for 100 nodes I'm not too sure. Are you expecting to implement VOIP?
>
> Cisco has some pretty good, somewhat dated, networking docs you may
> want to look at:
> http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\_doc/lanswtch.htm
> http://www.cisco.com/univercd/cc/td/doc/cisintwk/idq4/nd2012.htm
> http://www.cisco.com/univercd/cc/td/doc/cisintwk/idq4/index.htm
> http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\_doc/index.htm
> http://www.cisco.com/univercd/cc/td/doc/cisintwk/index.htm
>
> hth,
> prg
>
```