

Re: Single domain two IP subnets

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2006-09/msg00086.html>

- *From:* "Kurt" <lorentzenkurt@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 14 Sep 2006 21:06:49 -0700
-

No, subnets in IP are far more than purely logical.

They practically always represent a distinct "Broadcast domain" (area in which a broadcast will freely propagate).

Not if they're on the same wire. Although IP broadcasts will be discarded at the layer-3 level, Ethernet broadcasts propagate to every node in the broadcast domain (not to be confused with collision domain), regardless of IP subnet.

If two machines are on the same broadcast domain they are (practically*) always on the same subnet, and conversely if they are not on the same broadcast domain then they are not in the same broadcast domain.

Once again, does not apply if they are on the same wire.

[* It is theoretically possible to have multiple subnets on the same 'wire' or 'broadcast domain' but this is not a common practice in modern networks -- and still requires some special configuration.]

requires no special configuration at all. Get a switch, plug 4 computers into it. Put 2 on one IP subnet and two on another. Computers on the same IP subnet can talk, computers on disparate IP subnets cannot (at layer-3). But if you sniff the wire at any computer, you'll see arp broadcasts and such from every computer.

Re: Single domain two IP subnets

The real problem is many the incomplete understand of of VLANs switches, and switches in general, by many people.

One cannot understand VLANs (or any switches) completely without first understanding the differences and features of both Routers and Bridges -- we can call the features something else but switches are merely "switching" combined with either the Bridge or Router concept, or in modern devices a hybrid of all three concepts.

True, but I must say that I don't fall into that category. As the senior engineer/primary designer of a metro ring infrastructure, I live and breathe VLANs and routers every day of my life. They are what make shared ethernet infrastructures work.

VLANs switches allow the admin to (easily) redefine each bridged segment to include arbitrary connections to the switch, and thus map a "set of computers" to either one bridged broadcast domain OR another to which routing is required.

VLANs can exist as port based, protocol based even application based on really sophisticated multi-layer switches. They can live on a single switch, or span multiple switches, indeed multiple cities and service providers (although the latter is uncommon). Switches create separate collision domains. VLANs create separate broadcast domains. Communication between VLANs is not possible unless it is routed (OK, you could bridge it, but that would defeat the whole purpose).

Routed segments REQUIRE different IP subnets while EACH bridged segment typically (and all modern networks) place all of the machines on the same subnet.

That's the way it usually works, but the OP does not mention anything but IP subnets – purely logical separation.

Anybody could just change their IP address, or introduce a laptop with an IP address on another subnet and be connected.

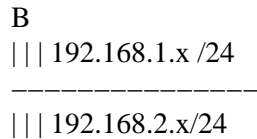
Re: Single domain two IP subnets

This really has nothing specific to do with VLANs per se.

It has nothing to do with a VLAN at all as a standalone statement. Incorporating VLANS into a single physical infrastructure enhances the security and prevents broadcast traffic between virtual segments. It really comes down to what the OP was driving at.



Those are two physical segments (and must be configured as different logical subnets in order to route traffic between).



If a plain 'ole \$99 switch is used, you have two logical subnets but one broadcast domain. I could still stick a 2 port router on there and route traffic between logical subnets. But if I use a managed switch and create two VLANs, I effectively have the same separation as "A".

It is a feature of whether that wiring segment is either Bridged or Routed.

Or virtually segmented and routed.

The KEY to a VLAN switch is the "area" or the "component network cables" which are BRIDGED vs. ROUTED can be configured by the Admin using switch-commands.

VLANs contain broadcasts and prevent any kind of connection between subnets other than through the router (which can be locked down as tightly as local management sees fit). If I were designing this for a client, I would probably sell them managed layer-2 switches for subnets

Re: Single domain two IP subnets

B-D and a layer-3 switch for Subnet A. Traffic from the other subnets could be trunked through the uplink port and routed at the L-3 switch. Quick to set up, central management, fewer devices to configure, plus L-3 switches will forward gigabit traffic at wire-speed unlike plain vanilla routers.

The above has little to do with understanding the basic concepts that are being confused here -- and detracts from keeping the explanation simple and accurate.

Perhaps, but the OP only mentioned IP subnets, no physical separation. Still, none of the answers provided a workable solution .

"Why 3 NIC in the router? No point in even connecting Subnet C if it is NOT going to communicate. <GRIN>"

Subnet C DOES have to communicate – With the DNS server / DC in subnet A – but not with computers in other subnets.

If this is a homework question it is , like most, poorly written. The "right" answer is probably to put a router between Subnets A, B, and D and leave subnet C all to itself. Of course the domain would not function on subnet C because it couldn't contact the DC or DNS server. So I proposed a solution that would allow subnet C to talk to the DC/DNS server but not communicate with other computers. The VLAN thing was in response to Lanwrench's post and took it a bit further.

But I stand my ground on these points: IP subnets are purely logical things. They can be configured without regard to the physical device or how it is cabled. Routers can route between IP subnets on the same physical segment or on separate physical segments, or on separate virtual segments.

....kurt

.