Notizen zu VLANs

Felix J. Ogris

19. Januar 2003

Virtual Local Networks, kurz: *VLANs*, können bei Faulheit zum Kabelverlegen oder bei gewachsenen Netzwerkstrukturen helfen.

Ein herkömmlicher Switch leitet *Broadcasts* („ein Host an alle“) an alle Ports weiter, außer natürlich an den, auf dem er den jeweiligen Broadcast empfangen hat; man sagt dann auch: Alle Ports eines Switches gehören zu einer *Broadcast Domain*. Ein VLAN-fähiger Switch kann hingegen einzelne Ports oder Portgruppen zu einer eigenen Broadcast Domain, sprich zu einem VLAN zusammenfassen, so daß Broadcasts nur noch Hosts in demselben VLAN erreichen. VLAN-Switches untereinander multiplexen die Datenströme auf eine Leitung, so daß sich VLANs auch auf mehrere Switches ausdehnen können. Nützlich ist dies, wenn sich mehrere Broadcast Domains (z.B. IP-Subnetze) über eine große räumliche Distanz erstrecken, z.B. viele Etagen eines Gebäudes, und sich auf jeder Etage Hosts für jede Domain befinden. Normalwerweise müßte man für jedes Netz eines eigenes Kabel verlegen. Setzt man VLANs ein, so werden die Switches einfach untereinander verbunden und für jedes Netz ein eigenes VLAN eingerichtet. Somit können sich die einzelnen Netze auf einer Etage nicht gegenseitig beeinflussen, obwohl sie an einem Switch hängen. Mit Routern, die ebenfalls Broadcast Domains begrenzen, wäre so etwas nur schwer möglich: Zum einen wird ein komplexeres IP-Setup nötig, zum anderen sind Router langsamer als Switches. Dennoch wird iweiterhin ein Router benötigt, der die einzelnen VLANs verbindet.
VLANs werden meistens unter Argumenten wie Zugewinn an Sicherheit oder Flexibilität verkauft; das ist weitestgehend sinnfrei. VLAN-fähige Switches können Verkehr auf einzelnen Portgruppen voreinander schützen; das ist deren Hauptaufgabe und kein Sicherheitsfeature. Der Netzwerk-Admin muß außer der IP- und der MAC-Adressenebene noch eine VLAN-Zugehörigkeit bedenken. Zusätzlich kennt ein Switch zwei Möglichkeiten, die VLAN-Zugehörigkeit eines Hosts festzulegen:

statisch Port X gehört zu VLAN Y; administrativer Aufwand, wenn ein Rechner umzieht

dynamisch aufgrund der MAC- oder IP-Adresse oder eines *Tags* zwischen MAC und IP legt ein Host seine Zugehörigkeit selbst fest; sicherheitstechnisch für die Tonne