11.09.2006

Benjamin Benz, Lars Reimann

VLAN: Virtuelles LAN

Netze schützen mit VLANs

Virtuelle Netze (VLANs) erlauben es, professionelle Sicherheitsstrategien sogar mit kleinem Budget auch im privaten Bereich umzusetzen. Ein managebarer Switch und ein PC als Router reichen schon aus, um das eigene Netz in verschiedene, voreinander geschützte Zonen zu unterteilen.

Selbst das heimische Netz braucht ein gewisses Maß an Sicherheit. Ungebetene WLAN-Gäste möchte man nicht jedes Paket im internen Netz sehen lassen. Die Viren- und Würmerschleuder der Kinder soll nicht gleich das ganze Netz erreichen – der Heimarbeitsplatz muss vor solchen Attacken geschützt sein. Eine DSL-Flatrate lädt dazu ein, sogar die eigene Webseite selbst zu hosten. Aber weiter als bis zum Webserver soll ein Besucher dann doch nicht vordringen.

VLANs bieten eine kostengünstige Alternative zur Einrichtung physikalisch getrennter Netze mit mehreren Switches. Ein gut konfigurierter VLAN-Switch verwaltet verschiedene Zonen und lässt jeden PC nur mit ausgewählten Partnern kommunizieren. Ist das Betriebssystem eines Rechners in der Lage, selbst mit VLAN-Informationen umzugehen, kann man über ein einziges Kabel zum Switch mehrere Netze erreichen.

Hubs und Switches verbinden in einem lokalen Netzwerk (Local Area Network, LAN) alle Rechner direkt miteinander. So kann zwar jedes Gerät mit den anderen kommunizieren, empfängt aber auch deren Rundsprüche. Ist dies aus Sicherheits- oder Performance-Gründen unerwünscht, unterteilt man das Netz in verschiedene Segmente.

Beim klassischen Ansatz bekommt jedes Subnetz einen eigenen Switch, und ein Router vermittelt zwischen den Bereichen. Jedes Subnetz hat einen eigenen IP-Adressraum und wenn nötig eigene Infrastruktur wie DHCP- oder Domainserver. Mit VLANs (Virtual Local Area Networks) geschieht diese Trennung nicht auf physikalischer, sondern logischer Ebene. Alle Ethernet-Pakete bekommen eine Markierung, die VLAN-Tags, anhand derer die Switches die Gruppenzugehörigkeit erkennen. Einzelne Rechner können auch mit mehreren Zonen kommunizieren.

Musterhaus

Die Vorteile von VLANs zeigt das Beispiel eines kleinen heimischen Netzes: Der Internet-Zugang über DSL soll allen Rechnern zur Verfügung stehen. Für den privaten Webauftritt und den Austausch von Dateien mit Freunden sorgt ein Server, dessen Dienste der Router über Port-Forwarding zugänglich macht. Den Familienmitgliedern stehen zum Surfen und Spielen zwei fest verkabelte PCs und ein Notebook zur Verfügung. Dieses überträgt seine Daten per WLAN ins Hausnetz. Besonderen Schutz erfordert der Heimarbeitsplatz (PC 3), der geschäftskritische Daten mit dem Arbeitgeber austauscht. Würmer und Viren, mit denen sich die anderen PCs eventuell infizieren, sollen ihm nichts anhaben können. Die IP-Adressen vergibt ein DHCP-Server auf dem Router.

Um den Webserver sicher zu betreiben, müsste er eigentlich in einer demilitarisierten Zone (DMZ) stehen. Dazu würde der Router eine eigene Netzwerkkarte benötigen. Ebenfalls problematisch ist die Anbindung des Access-Points, der alle Pakete aus dem WLAN an das LAN weiterreicht; er arbeitet standardmäßig als Bridge und spiegelt alle Pakete zwischen den beiden Netzen. So kann zwar das Notebook auf alle Freigaben der anderen Rechner zugreifen, ein Angreifer, der erfolgreich die WLAN-Verschlüsselung umgangen hat, aber auch. Außerdem erhält jeder Rechner alle Rundspruchpakete (Broadcasts); dadurch kann bei größeren Installationen ziemlich viel Last auftreten. Den Datenverkehr zwischen zwei Partnern hingegen sehen die anderen im Normalfall nicht, da der Switch für jeden Port eine eigene Collision-Domäne verwaltet; Hubs tun dies nicht. Mit bestimmten Angriffen wie ARP-Spoofing oder MAC-Flooding kann man aber auch einen Switch dazu bringen, Pakete an falsche Ports auszuliefern.

Innenausbau

Für das Beispielnetz ist eine Unterteilung in vier getrennte Zonen wünschenswert: Der Server kommt in eine DMZ, der WLAN-Access-Point in einen gesonderten Bereich und der Heimarbeitsplatz wird vom Rest der PCs getrennt. Hierzu ist lediglich ein VLAN-tauglicher, managebarer Switch nötig, der ungefähr 100 bis 150 Euro mehr kostet als ein einfaches Modell. Er übernimmt die Trennung in verschiedene VLANs. Dazu stehen verschiedene Verfahren zur

Auswahl: portbasierte Aufteilung und VLAN-Tagging nach dem **IEEE-Standard 802.1Q[1]**.

Das ältere und einfachere Port-VLAN teilt jeden Port fest einem einzelnen Netzsegment zu. Alle Ports im selben Segment bilden eine Broadcast-Domäne, so als würden sie an einem eigenen normalen Switch hängen – sie erhalten also alle Rundspruchpakete (Broadcasts), aber nicht alle Datenpakete; das wäre nur in einer Collision-Domäne der Fall. Kein Port kann in mehr als einem Netz sein. In dem Beispiel müsste der Router eine eigene Netzwerkkarte für jedes der vier VLANs besitzen. Die VLAN-Verwaltung bleibt dabei auf einen einzelnen Switch beschränkt.

Etikette

Flexibler sind VLANs, die Informationen in den Ethernet-Frames nutzen. Der Standard **802.1Q[2]** sieht dazu zwischen Adress- und Längenfeld jedes Ethernet-Pakets vier zusätzliche Bytes vor. Die ersten beiden (Tag Protocol Identifier) kennzeichnen mit dem festen Wert 0x8100 das Vorhandensein der 802.1Q-Erweiterung. Die restlichen zwei Bytes (Tag Control Information) setzen sich aus drei Bits für die Priorität (Class of Service, CoS), einem Bit namens Canonical Format Indicator (CFI) und zwölf Bits für die VLAN-ID (VID) zusammen.

Ein VLAN-Switch benutzt diese VID, um zu entscheiden, an welchen anderen Port er das Paket weiterleiten darf. Empfängt er ein normales, nicht markiertes Ethernet-Paket, so verpasst er ihm ein Tag mit der dem jeweiligen Port zugeordneten VID. Von Geräten an speziellen Tagged-Ports akzeptiert der Switch auch bereits markierte Pakete. Dadurch kann man mehrere Switches kaskadieren.

Moderne Betriebssysteme können die Frames selbst mit Tags versehen und emulieren so mehrere LAN-Schnittstellen. In unserem Beispiel vermittelt der Router zwischen den vier VLANs und dem Internet. Da er die VLANs selbst taggen und zuordnen kann, braucht er dafür nicht vier Netzwerkkarten, sondern nur eine einzige. Ein Anschluss am Switch darf dafür auch zu mehreren VLANs gehören.

Anhand des CoS kann ein Switch wichtige Pakete (hoher CoS-Wert) bevorzugt behandeln. Dies geschieht unabhängig von QoS-Regeln, die auf höheren OSI-Protokollschichten arbeiten. Das CFI dient zur Kompatibilität mit Token-Ring-Topologien und hat bei Ethernet immer den Wert Null. Von den 4096 möglichen Kombinationen für die VID sind die oberste und unterste Adresse reserviert.

Cui bono

In größeren Netzen spielen die Anzahl der Switches oder die gesparten Netzwerkkarten keine große Rolle. VLANs kommen dort hauptsächlich zur besseren Strukturierung der Netztopologie zum Einsatz. Sie erlauben es, die Zuordnung von Rechnern zu Netzen nicht mehr nach geografischen, sondern nach thematischen Gesichtspunkten vorzunehmen – ohne dabei riesige Mengen an Kabeln zu verlegen. Der Mitarbeiter aus der Buchhaltung mag zwar direkt neben dem Entwickler sitzen, braucht aber Zugriff auf sensible Daten, die andere Mitarbeiter nichts angehen. Ein VLAN-Switch kann so beide Arbeitsplätze den richtigen Netzen zuordnen und die Daten über einen gemeinsamen Backbone weiterleiten.

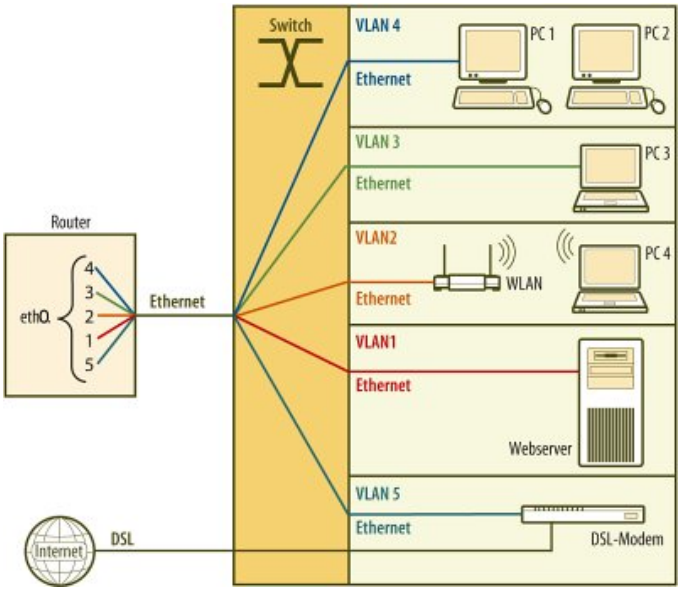
Außerdem sind Umzüge unproblematisch: Eine Änderung in der Switch-Konfiguration reicht aus, die Verkabelung bleibt gleich. Für größere Installationen beherrschen manche Switches Protokolle (GARP VLAN Registration Protocol, andere proprietär), mit denen sie ihre jeweiligen VLAN-Konfigurationen untereinander abgleichen können. Layer-3-Switches können zusätzlich zu den 802.1Q-Tags noch Informationen aus höheren OSI-Schichten hinzuziehen, um Pakete effizient zu vermitteln.

Aufpassen muss man allerdings mit älterer Hardware, denn diese kommt nicht immer mit den überlangen getaggten Ethernet-Frames klar. In diesem Fall muss der Switch die VLAN-Tags wieder entfernen, bevor er sie an die Zielgeräte ausliefert. (Für eine erweiterte Lösung siehe weiter unten).

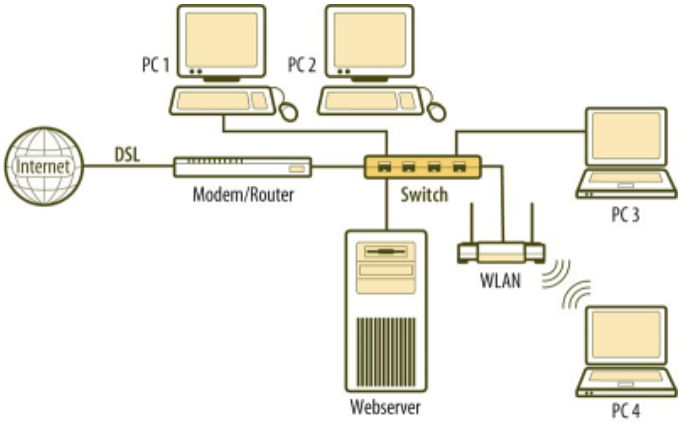
Die enorme Flexibilität bei der Zuordnung von PCs zu Netzen vereinfacht auch die Performance-Optimierung: Eine alte Faustregel besagt, dass im optimalen Netz 80 Prozent des Netzwerkverkehrs innerhalb des Subnetzes und nur 20 Prozent über Netzgrenzen hinweg läuft. Zu viele Rechner im selben Subnetz bremsen sich aber durch häufige Rundsprüche (Broadcasts) gegenseitig aus.

Sicherheitsplanung

Eine kleine Analyse des vorhandenen Netzes oder der möglichen Erweiterungen hilft bei der Planung und Umsetzung einer Netztopologie mit virtuellen Subnetzen. Das eingangs beschriebene Heimnetz mag als Beispiel dienen. Das DSL-Modem ist über Ethernet angebunden, darf aus Sicherheitsgründen aber nicht im selben Netz hängen wie die Client-PCs. Ein selbst gebauter Router soll zwischen dem LAN und dem Internet vermitteln.

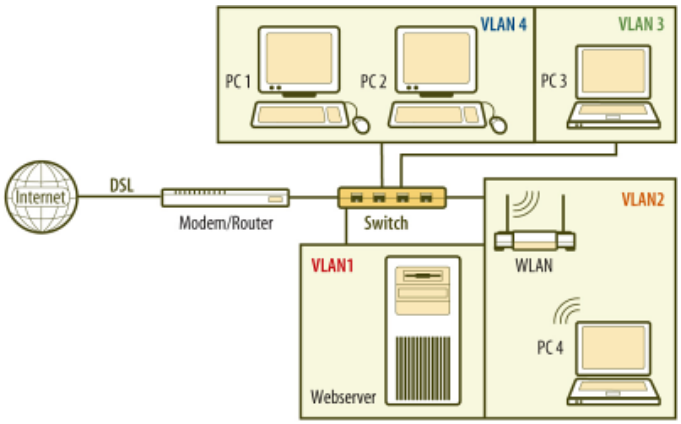


Der Router bekommt als einziger Rechner die Ethernet-Pakete mit VLAN-Tags. So kann er mit einer Netzwerkkarte zwischen allen virtuellen Netzen vermitteln.



Klassisches Netz: Der Switch vermittelt zwischen allen Komponenten im Netzwerk. Jeder Rechner kann mit jedem kommunizieren – Würmer können sich problemlos verbreiten.

Auf dem Router soll wahlweise Linux oder Windows XP laufen. Der administrative Zugriff auf diese Maschine ist so weit beschränkt, dass sie als vertrauensvoll einzustufen ist. Um Kosten zu sparen, soll sie nur eine Netzwerkkarte bekommen und dank VLAN-Tagging dennoch alle virtuellen Subnetze erreichen. Alle anderen Rechner gelten als nicht vertrauenswürdig und überlassen dem Switch das Zuordnen der VLAN-Tags. Da zwei Geräte (Router und Switch) VLAN-Tags vergeben, und die Konfiguration flexibel und erweiterbar sein soll, fällt die Wahl auf ein VLAN nach dem IEEE-Standard **802.1Q[3]**.

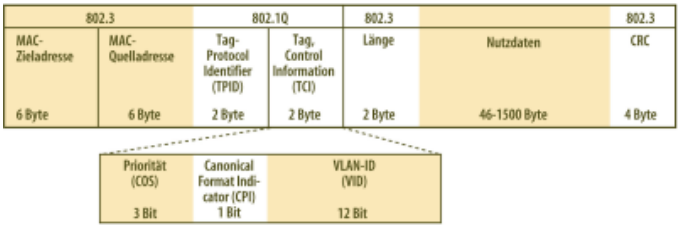


Zonenmodell: Ein VLAN-tauglicher Switch kann das Netz so in Subnetze unterteilen, dass nur noch Rechner innerhalb einer Zone direkt miteinander kommunizieren können. Dazwischen vermittelt ein Router.

Insgesamt fünf VLANs sollen entstehen, in denen der Router mit jeweils einem unabhängigen Interface hängt: Eines, um den Webserver vom internen Datenverkehr abzutrennen – die IP-Adresse des Servers ist statisch, damit ein Port-Forwarding zu ihm einfacher ist. Das zweite Netz verbindet den Router mit dem Access-Point. Auf diesem virtuellen Interface soll der Router per DHCP IP-Adressen zuweisen, damit das Notebook sich bequem einbuchen kann. Dasselbe gilt für VLAN4, das die beiden Surf-PCs ins Internet bringt. Das vierte Netz lässt nur den Heimarbeitsplatz ins Internet und enthält ebenfalls nur ein Gerät. Auch das DSL-Modem hängt am Switch – in einem eigenen VLAN. Das spart die sonst zur sauberen Trennung von LAN und Internet nötige zweite Netzwerkkarte im Router ein und erlaubt es, Modem und Router räumlich zu trennen. Das Ganze verhält sich dann so, als ob fünf Switches vorhanden wären. Daher braucht jedes dieser virtuellen Subnetze einen eigenen IP-Adressraum.

Wunschzettel

Ein passender Switch kostet zwischen 150 und 300 Euro und bringt meist 16 oder 24 Ports mit – für den Heimgebrauch sicher mehr als ausreichend. Achtung, einigen günstigen VLAN-Switches fehlen Konfigurationsoptionen, um wichtige Sicherheitslücken zu schließen (siehe Kasten VLAN Security) – von solchen Geräten sollte man zu Gunsten der Netzwerksicherheit die Finger lassen. Ein Blick in die meist online verfügbaren Handbücher zeigt, welche Einstellmöglichkeiten ein Switch bietet. Die Netzwerkkarte des Routers muss ebenfalls mit dem 802.1Q-Protokoll zurechtkommen. Für die meisten modernen 100-MBit-Karten stellt dies keine Hürde dar, ältere 10-MBit-Modelle scheiden hingegen aus. Da Windows XP die Behandlung von VLANs weitgehend dem Treiber überlässt, ist bei der Hardware-Auswahl ein wenig Recherche nötig. Gute Software-Unterstützung gibt es derzeit für Karten von Intel. Linux-Nutzer haben es deutlich leichter, denn dort kümmert sich der Kernel selbst um die virtuellen Netze, ein hardwarespezifischer Treiber ist nicht nötig. Da der Switch die VLAN-Tags wieder entfernt, bevor die Datenpakete bei den Client-PCs und dem WLAN-Access-Point ankommen, bestehen keine besonderen Anforderungen an deren Ethernet-Hardware.

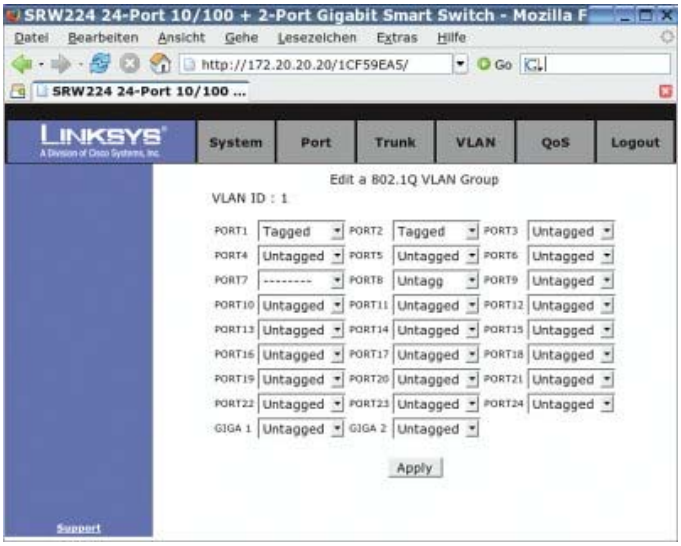


Die VLAN-Tags verlängern den Ethernet-Frame um vier Byte. Daran kann sich ältere Hardware schon mal verschlucken.

Um das Netz möglichst flexibel zu halten, bietet sich Tag-basiertes VLAN nach IEEE 802.1Q an. Andere, teilweise proprietäre Verfahren der Switch-Hersteller, etwa Zuordnung der Zonen über nicht fälschungssichere MAC-Adressen, lohnen nur selten. Bei 802.1Q wählt man für jeden Port des Switches aus, ob dort bereits getaggte Pakete von 802.1Q-konformen PCs und anderen Switches eintreffen, oder ob der Switch die Pakete neu markieren soll. In diesem Fall erweitert er alle eingehenden Ethernet-Frames um eine VLAN-ID und entfernt diese bei ausgehenden wieder. Daraus ergeben sich zwei Vorteile: Die Integration älterer Hardware ist unproblematisch, da die überlangen Frames sie überhaupt nicht erreichen. Außerdem bleibt die Kontrolle über die Tag-Vergabe auf den Switch und einige ausgewählte vertrauenswürdige Rechner wie die Firewall beschränkt.

Drehkreuz

Wir haben für den Testaufbau einen 24-Port-Switch von Linksys (SRW224) verwendet. Zusätzlich zu den 100-MBit-Ports besitzt er zwei Gigabit-Links und kostet rund 230 Euro. Die Konfiguration erfolgt entweder über ein Web-Interface oder die serielle Konsole. Leider stehen nicht alle Optionen auf jedem der beiden Frontends zur Verfügung – VLAN-Einstellungen sind nur per Weboberfläche möglich. Auf welcher IP-Adresse der Switch lauscht, verrät das Handbuch, bei unserem Modell war es die 172.20.20.20.



Bei VLAN-Switches legt man für jeden Port fest, ob er getaggte Pakete entgegennehmen darf. Steht der Port auf untagged, so entfernt der Switch die VLAN-Markierungen ausgehender Pakete.

Der Linksys-Switch bietet auf der Konsole zwar keine Einstellmöglichkeiten für VLANs, dafür aber wichtige Sicherheitseinstellungen - ein ungesicherter Switch macht alle Sicherheitsanstrengungen auf höheren Ebenen zunichte.

Für die serielle Schnittstelle legt Linksys ein Nullmodemkabel bei. Ein geeignetes Terminalprogramm bringt Windows mit: Im Startmenü findet sich unter Zubehör/Kommunikation das HyperTerminal. Bei der Einstellung der Kommunikationsparameter hilft das Handbuch weiter. 19 200 Bit/s, acht Datenbits, ein Stoppbit und keine Parität (8N1). Steht die Verbindung, öffnet der Switch auf ein Enter-Zeichen hin seine Oberfläche und fragt nach Benutzernamen und Kennwort. Dieses sollte man dann auch als Erstes ändern, um möglichen Angreifern, die üblicherweise die ab Werk eingestellten Kennungen wissen, den Zugriff auf den Switch zu verwehren.

Die physikalische Schnittstelle eth0 darf keine IP-Adresse bekommen, denn sie versendet weiterhin ungetaggte Pakete – die Kommunikation erfolgt über die virtuellen Schnittstellen.

Aktiviert man VLAN nach 802.1Q, bekommen alle Ports die VLAN-ID (VID) 1 und den Modus untagged. Es ändert sich auf den ersten Blick also nichts, jedes Gerät kann weiterhin mit jedem anderen kommunizieren, und die überlangen Ethernet-Frames verlassen den Switch nicht.

Für das Beispielnetz bietet sich folgende Konfiguration an: Der Router an Port 1 darf als einziger 802.1Q-Frames senden und empfangen – daher bekommt er den Tagged-Modus. Alle anderen bleiben im Untagged-Betrieb. Ports, die nicht verwendet werden, deaktiviert man oder gibt ihnen eine unbenutzte VID. Angreifer können so nicht in andere Netze hineinhorchen. Die Zuordnung der VIDs auf die restlichen Ports zeigt die Tabelle. Der Tagged-Port, an dem der Router hängt, bekommt alle anderen VIDs zugewiesen. So kann er zwischen den Zonen vermitteln.

Linux

Linux bringt weitreichende Unterstützung für VLANs mit, diese ist aber in den Kernels mancher Distributionen nicht aktiviert. Die Existenz des Verzeichnisses /proc/net/vlan zeigt die 802.1Q-Unterstützung an – eventuell muss vorher das Modul 8021q geladen werden. Sowohl bei Suse 9.2, Debian-Sarge als auch bei Fedora Core 3 kommen alle nötigen Pakete mit der Distribution.

Die Mehrkosten für einen VLAN-Switch rentieren sich schnell: Er erhöht die Sicherheit im Netz deutlich und hilft, den Aufwand bei Verkabelung und Netzverwaltung zu reduzieren.

Fehlen sie, so muss man die Kernelquellen installieren und einen eigenen Kernel bauen: Zuerst passt ein make oldconfig die Quellen an die Einstellungen des laufenden Kernels an – somit funktioniert mit dem neuen Kernel alle Hardware weiter. Dann ruft man mit make xconfig oder make menuconfig das Konfigurationsskript des Kernels auf. Dabei kann es je nach Distribution vorkommen, dass einige Entwicklerpakete fehlen, die man dann nachinstallieren muss.

Im Menüpunkt "Device drivers/Networking support/Networking options" aktiviert ein Haken bei "802.1Q VLAN Support" die virtuellen Netze. Nun übersetzt ein `make` den Kernel und seine Module. Die Befehle `make install` und `make modules_install` kopieren den frisch übersetzten Code an die passenden Stellen im Dateisystem. Je nach Bootmanager und Distribution sind noch weitere Schritte erforderlich. Für den älteren 2.4er-Kernel bietet www.candelatech.com die **offiziellen Kernel-Patches[4]** an.

Zur Konfiguration dient das Programm `vconfig` (Suse: vlan-xx.rpm), das ebenfalls www.candelatech **zum Download[5]** anbietet. Es verwaltet die virtuellen Schnittstellen und teilt dem Kernel mit, als welche Devices er sie

einblenden soll. So ordnet der Befehl

```
vconfig add eth0 1
```

das erste virtuelle Netz mit der VID 1 (für den Webserver) der Netzwerkkarte eth0 zu. Es steht dann als eth0.1 allen Linux-Programmen zur Verfügung. Da manche Switches mit der VID 1 Probleme haben, muss man eventuell die Nummerierung bei 2 beginnen. Falls mehrere Karten im PC stecken, helfen die Kommandos `ifconfig`, `lspci` und `lsmod`, die gewünschte Karte anhand von MAC-Adresse, PCI-ID oder geladenem Treiber zu finden.

Die IP-Adresse weisen entweder ein

```
ifconfig eth0.1 192.168.1.1
```

oder die Tools der jeweiligen Distribution der virtuellen Schnittstelle zu. Die physikalische eth0, die ungetaggte Pakete verschicken würde, bekommt keine IP zugewiesen. Ein `ifconfig eth0 0.0.0.0` stellt dies sicher. Die anderen vier VLANs richten die Befehle

```
vconfig add eth0 2
vconfig add eth0 3
vconfig add eth0 4
vconfig add eth0 5
```

ein. Die Zuteilung der IP-Adressen auf dem Router geschieht auch für diese Interfaces manuell:

```
ifconfig eth0.2 192.168.2.1
ifconfig eth0.3 192.168.3.1
ifconfig eth0.4 192.168.4.1
ifconfig eth0.5 192.168.5.1
```

Hausnetz

	Router	DSL	PC4	PC3	PC2	PC1
Server	VID1	-	-	-	-	-
PC1	VID2	-	-	-	VID2	
PC2	VID2	-	-	-		
PC3	VID3	-	-			
PC4	VID4	-				
DSL	VID5					
- keine Verbindung						

IP-Adressräume

	Netz	Router	Clients
VLAN1	192.168.1.0/24	192.168.1.1	Webserver: 192.168.1.2
VLAN2	192.168.2.0/24	192.168.2.1	PC4:192.168.2.2
VLAN3	192.168.3.0/24	192.168.3.1	PC3:192.168.3.2
VLAN4	192.168.4.0/24	192.168.4.1	PC1:192.168.4.2, PC2:192.168.4.3
VLAN5	192.168.5.0/24	192.168.5.1	DSL-Modem: 192.168.5.2

Sobald man den Client-Rechnern und dem Webserver eine IP aus dem jeweiligen Netz zugewiesen hat, kann man mit dem Programm ping die Installation testen. Auf den Befehl (Windows-Eingabeaufforderung von PC1)

```
ping 192.168.4.3
```

sollte die Ausgabe ungefähr so aussehen:

```
Antwort von 192.168.4.3: Bytes=32  Zeit<1ms TTL=30
```

Die Gegenprobe, von PC1 zum Webserver, sollte auch dann fehlschlagen, wenn man PC1 temporär eine IP aus dem Subnetz des Servers gibt. Eine Kommunikation zwischen den Zonen und ins Internet ist mit dieser Konfiguration allerdings noch nicht möglich. Dazu fehlen noch einige Firewall- und Routing-Einstellungen auf dem

Server. Da sich diese nicht von Installationen ohne VLANs unterscheidet, zeigen wir hier nur eine nicht unbedingt sichere Minimallösung. Zuerst die iptables-Regeln für den Internet-Zugang – wir gehen dabei davon aus, dass ein vorhandener DSL-Router über die IP 192.168.5.2 erreichbar ist:

```
iptables -P FORWARD DROI
iptables -A FORWARD -o eth0.5 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0.5 -j MASQUERADI
echo "1" > /proc/sys/net/ipv4/ip_forwarc
route add default gw 192.168.5.2
```

Mit diesen Regeln dürfen alle Clients alle Internet-Dienste nutzen. Gegenseitig erreichen sie sich jedoch nicht. In der Praxis sollte man das Regelwerk deutlich strikter halten und genau an die eigenen Bedürfnisse anpassen.

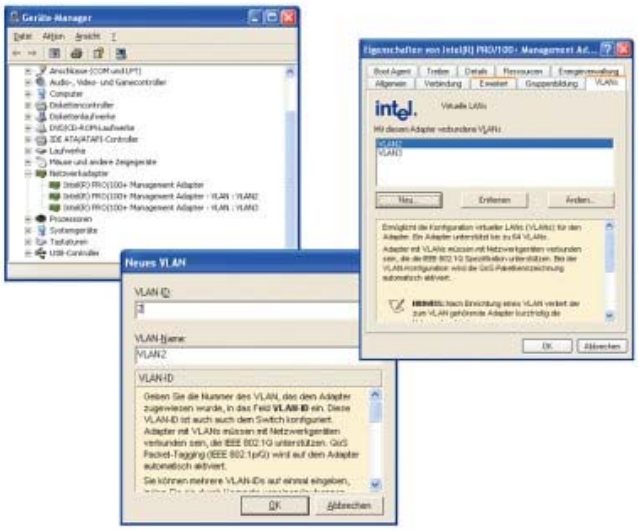
Komfortabler wird die Administration der Clients beim Einsatz eines DHCP-Servers. Dieser weist ihnen IP-, Gateway- und DNS-Adressen zu. Dafür muss man ihm lediglich mitteilen, auf welchen Schnittstellen er überhaupt auf DHCP-Anfragen lauschen soll (/etc/sysconfig/dhcpd). Für jedes der vier Netze legt ein eigener Eintrag in der Datei dhcpd.conf den IP-Bereich fest:

```
subnet 192.168.2.0 netmask 255.255.255.0 {
  range 192.168.2.2 192.168.2.100;
  option routers 192.168.2.1;
}

subnet 192.168.3.0 netmask 255.255.255.0 {
  range 192.168.3.2 192.168.3.100;
  option routers 192.168.3.1;
}
```

Windows

Windows XP überlässt die Verwaltung von VLANs dem Treiber der Netzwerkkarte. Daher ist bei der Auswahl der Karten für einen Rechner, der selbst taggen soll, Vorsicht geboten. Gute Erfahrungen haben wir mit Netzwerkadaptern von Intel (PRO 100, PRO 1000) und den etwas veralteten Treibern der 8er-Version gemacht. Das hauseigene Tool ProSet liegt diesen bei und führt grafisch durch die Konfiguration. Nach dem Aufruf über einen Doppelklick auf das Symbol in der Taskleiste muss man zuerst das 802.p-Tagging (QoS) aktivieren, denn dahinter verstecken sich auch die IEEE-802.1q-Erweiterungen. Danach fügt man über das Menü einzelne VLANs hinzu. Die IP-Adresse vergibt man, wie bei Windows üblich, in den Eigenschaften der Netzwerkumgebung – dort taucht für jedes VLAN eine eigene virtuelle Netzwerkkarte auf.



Windows überlässt die VLAN-Verwaltung den Hardware-Treibern: Die Intel-ProSet-Treiber simulieren für jedes VLAN eine eigene Netzwerkkarte.

Problematisch ist hingegen der Einsatz jüngerer Treiber. Die Version 9.1 verlagert die ProSet-Tools in den Gerätemanager. Dort tauchen sie allerdings nur auf, wenn das Multi-Language-Pack installiert ist. Bei der

Installation gibt es Fallstricke: Zuerst muss man alle alten Treiber restlos deinstallieren oder am besten mit einer jungfräulichen Windows-Installation beginnen. Nach dem Herunterladen des ProSet-Treibers entpackt man ihn, darf ihn aber keinesfalls installieren. Danach holt man das Multi-Language-Pack für ProSet und extrahiert es in dasselbe Verzeichnis. Erst dann folgt der Aufruf des Installationsprogrammes. Mit etwas Glück zeigt das Fenster mit den Eigenschaften der Netzwerkkarte jetzt mehrere neue Registerkarten an, unter anderem auch mit den VLAN-Optionen.

Ausblick

Schon in einem relativ kleinen Netz kann die Unterteilung in verschiedenen VLAN-Zonen die Netzsicherheit deutlich steigern. Die Mehrkosten halten sich in Grenzen, besonders wenn man langfristig zur Trennung von Netzen mit mehreren Switches übergehen würde. Auch der Aufwand für die Installation ist dank der guten Linux-Unterstützung unproblematisch. Etwas unübersichtlich ist leider das Angebot an VLAN-tauglichen Switches. Denn die maximale Sicherheit erreicht nur ein Netz, in dem auch die Switches nicht durch Angriffe wie MAC-Flooding dazu zu bewegen sind, in einen Hub-Modus zurückzuschalten. Unabhängig von der Art des Netzaufbaus sind die Firewall-Regeln weiterhin der wichtigste Punkt bei der Netzwerksicherheit. Sie sollten nur wirklich benötigte Dienste zwischen den Subnetzen vermitteln. Getrennte Zonen auf dem Switch helfen nicht weiter, wenn die Firewall munter zwischen den Zonen Pakete vermittelt.

Da der Router in dem Beispiel nur eine einzige Netzwerkkarte nutzt, um fünf virtuelle Netze zu bedienen, teilen sich diese die vorhandene Bandbreite. Bei datenintensiven Anwendungen wie Fileservern lohnt sich hier eventuell eine Gigabit-LAN-Karte – vorausgesetzt, der Switch besitzt ebenfalls einen geeigneten Port. Ein solcher VLAN-Fileserver kann auch davon profitieren, dass der Datentransfer in verschiedene Subnetze nicht geroutet, sondern geswitcht wird. (**rek[6]**)

Literatur

1. Benjamin Benz, **Logische Netze, Virtuelle LANs unterteilen das Netzwerk in Sicherheitszonen, c't 1/05, S. 90[7]**
2. **IEEE 802.1Q Standard[8]**
3. Jörg Rech, Ethernet, Technologien und Protokolle für die Computervernetzung, Heise Verlag, ISBN 3-88229-186-9
4. **Basic Network Design: Issues and Answers[9]**

Sicherheits-Checkliste
Damit der Switch nicht die schwächste Stelle des Netzes bildet, sind auch mit VLANs einige Sicherheitseinstellungen nötig: Alle unbelegten Ports auf dem Switch sollte man abschalten und ihnen ein unbenutztes VLAN zuweisen. Aktive Ports, an denen ein Endgerät hängt, sind so zu konfigurieren, dass sie kein Trunking bei 802.1Q akzeptieren. Die Standardeinstellung beispielsweise bei Ciscos VTP ist auf Bequemlichkeit optimiert: Der Switch versucht automatisch zu erkennen, ob die Gegenseite ein solches Protokoll versteht, und aktiviert das passende Trunking-Protokoll selbstständig. Ein Angreifer, der einen Rechner dazu bringen kann, eine solche 802.1Q-Negotiation zu starten, bekommt so Zugriff auf alle VLANs.

Der Zugriff auf Konfigurationsschnittstellen muss mit einem Passwort gesichert werden. Andernfalls besteht die Gefahr, dass durch automatische Konfigurationsmechanismen wie GVRP oder VTP ein neu ins Netz gebrachter Switch sich als führender Konfigurationsverteiler aufspielt. Dann wird nicht die bestehende Konfiguration auf den neuen Switch kopiert, sondern die leere Konfiguration des neuen Switches auf alle produktiven Switches verteilt. Bei dieser Gelegenheit sollte man auf dem Neugerät auch das Cisco-spezifische Autodiscovery-Protokoll (CDP) deaktivieren – so bekommt ein Angreifer nicht gleich die Versionsnummern aller Geräte frei Haus.

In manchen Netzwerken – etwa der DMZ eines Firewall-Setups – kann es sinnvoll sein, ein VLAN als Private VLAN zu deklarieren. In einem solchen können die Endgeräte im selben VLAN nicht direkt miteinander reden, sondern müssen über den Router kommunizieren. Auf diese Weise ist auch innerhalb einer Broadcast-Domain eine vollständige Kommunikationskontrolle durch die Firewall möglich.

In einem Layer-2-Netzwerk aus Switches existiert ein Verteilbaum (Spanning Tree), der festlegt, auf welchen Wegen die Switches erreichbar sind. Das System, das die Wurzel dieses Verteilbaums ist, kann die Topologie des Restnetzes verändern. Indem man BPDU-Guard und Root-Guard aktiviert, schließt man dieses Einfallstor.

Schließlich ist durch den Einsatz von 802.1X möglich, Endgeräte durch Maschinen-Passwörter oder Public-Key-Zertifikate zu identifizieren. Switch-Ports werden nur dann aktiv, wenn an ihnen autorisierte Geräte hängen. Erweiterungen von 802.1X bieten außerdem die Möglichkeit, einem so angesteuerten Port automatisch das für diese Maschine zutreffende VLAN

zuzuweisen. In einem solchen Netz kann man einen beliebigen Rechner an jedem Port anschließen, und der Rechner befindet sich immer im passenden VLAN und ihm wird eine passende IP-Adresse zugewiesen. (Kristian Köhntopp)

VLAN Security

Angriffe gegen Switches mit VLANs kompromittieren die Sicherheit im Netzwerk auf Schicht zwei (OSI-Modell) und können daher Sicherheitsmaßnahmen auf allen

höheren Schichten aushebeln. Daher ist es schon bei der Planung von VLANs wichtig, Angriffe an dieser Stelle zu berücksichtigen und Gegenmaßnahmen vorzusehen.

Einer der einfachsten Angriffe gegen Switches – egal ob sie VLANs einsetzen oder nicht – lässt sich mit Werkzeugen wie macof oder dsniff umsetzen. Diese Werkzeuge generieren Pakete mit tausenden unterschiedlichen MAC-Adressen und bringen so die MAC-Tabelle des Switch zum Überlaufen. Der Switch kann sich in seinem begrenzten Speicher nicht mehr merken, welche MAC-Adresse hinter welchem Port angeschlossen ist und schaltet auf die nächstschlechtere Betriebsart herunter: Er wird zum Hub und kopiert alle Pakete zu allen Ports weiter – der Angreifer kann nun auch Pakete mitschneiden, die nicht für ihn bestimmt sind. Diese Fallback-Automatik muss man unbedingt deaktivieren.

Ungesicherte Trunking-Ports bieten ein weiteres Einfallstor: Der Angreifer gibt sich als Switch aus und tagged die Pakete selbst. Der echte Switch versucht nun, dieses neue Gerät zu integrieren und stellt ihm freundlicherweise alle VLANs mit IEEE 802.1Q Tags zur Verfügung.

Eine kompliziertere Variante dieses Angriffes sendet zweimal mit IEEE 802.1Q verpackte Pakete an einen Switch, der nur die äußere Verpackungsebene entfernt. Da der innere Frame nicht dieselbe VLAN-ID wie die äußere Verpackung enthalten muss, können Pakete dabei illegal von einem VLAN in das nächste überwechseln. Zum Glück erlaubt diese Art des Angriffes keinen Rückweg zum Angreifer.

Switches koordinieren sich untereinander über das Spanning Tree Protocol (STP), um das Netzwerk auch dann schleifenfrei zu halten, wenn die physische Verkabelung redundante Verbindungen enthält. Durch Angriffe auf STP-Ebene kann das Zusammenbrechen von bestehenden Verbindungen genauso signalisiert werden wie das Vorhandensein nicht vorhandener Links – der Angreifer kann sich so zur Root-Bridge im Switch-Baum machen und bekommt wahlweise alle Pakete im Netz zu sehen oder kann von seinem Platz aus das Netzwerk abhängen.

Gegen alle diese Angriffe existieren in neueren Switches Mechanismen, die das Netzwerk auch auf Schicht 2 sicher halten können. Leider sind diese Mechanismen per Default meistens abgeschaltet, weil ihr Einsatz die Kenntnis der gewünschten Netzwerktopologie und eine manuelle Abstimmung der Komponenten erfordert. Des Weiteren gehören Switches grundsätzlich in verschlossene Räume, denn solange jedermann nach Belieben den Switch und seine Verkabelung manipulieren kann, ist keine Sicherheit herstellbar. (*Kristian Köhntopp*)

URL dieses Artikels:
http://www.heise.de/netze/artikel/77832

Links in diesem Artikel:

[1] http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf
[2] http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf
[3] http://www.heise.de/kiosk/archiv/ct/05/01/090/
[4] http://www.candelatech.com
[5] http://www.candelatech.com
[6] mailto:rek@heise-netze.de
[7] http://www.heise.de/kiosk/archiv/ct/05/01/090/
[8] http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf
[9] http://www.cisco.com/warp/public/779/smbiz/netguide/v2_good_design.html