"VMPS" enviado por Navarro Andres

Enviado: lunes, 11 de diciembre de 2006, 23:33

VMPS

VLAN

Una red de área local (LAN) esta definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación.

Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN, como pueden ser los directivos de la misma, y que al estar todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no se aprovecha correctamente.

Por lo tanto, la necesidad de confidencialidad como el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs (Virtual LANs)

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados, como hubs, bridges, switches o estaciones de trabajo. La definimos como una subred definida por software y es considerada como un dominio de Broadcast en el que los dispositivos pertenecientes a este dominio pueden estar en el mismo medio físico o bien puede estar en distintos sectores de la corporación.

Dicho de otra manera, el fenómeno de la VLAN es un método de crear redes lógicas independientes dentro de la misma red física, a las que pertenecerán unos dispositivos específicos, no pudiendo comunicarse dispositivos de diferentes VLANs si no es a través de un router. Las VLANs funcionan en el nivel 2 del modelo OSI, aunques se suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3.

De esta manera, muchas VLANs (hasta 4096) pueden coexistir en una misma red. Esto tiene una gran ventaja y es que se reduce el dominio de broadcast, y administrativamente se separan lógicamente los segmentos de la LAN. Es una red de ordenadores conectados por medio del mismo cable, pero como si estuvieran conectados físicamente a diferentes segmentos de la red. Esta administración de la red se hace por software, y no por hardware, lo que lo dota de gran flexibilidad y comodidad.

Las VLANs se identifican por un número, el VLAN ID. Existen VLANs especiales:

La VLAN con ID 1 es la VLAN por defecto, yendo todo el tráfico que no tenga definida una VLAN por ella.

En equipos Cisco, las VLANs con IDs 1002-1005 están restringidas como VLANs por defecto para redes FDDI y Token-Ring.

Una de las ventajas mas grandes de las VLANs emerge cuando movemos físicamente un ordenador a otro sitio, puesto que puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración del hardware.

La trama 802.1q

Es un estándar de la IEEE para etiquetar tramas y de esta manera poder saber a que VLAN pertenece cada trama. Este estándar permite hasta 4096 VLANs. Se insertan 4 bytes de etiquetado en la trama principal de ethernet (entre los campos“dirección origen” y “tipo-longitud”)
y como la trama se ve alterada, se vuelve a calcular la secuencia FRC, antes de que se envíe la trama a través de el enlace “trunkeado”. En el contexto de VLANs, el termino trunking denota un enlace de red por el que están conectadas múltiples VLANs, y están identificados por etiquetas insertadas en sus paquetes (mediante 802.1q).

Esto resulta muy útil para interconectar varios switches a los que hay conectados diferentes dispositivos, habiendo dispositivos conectados a diferentes switches pero pertenecientes a la misma VLAN.

Otra utilidad es la aplicación de este mecanismo directamente sobre los ordenadores, lo que permite enviar el tráfico por distintas VLANs según por ejemplo, el usuario que utilice el equipo, o la aplicación o cualquier otra dependecia, lo que permite una gran flexibilidad. Este mecanismo viene ya implementados en sistemas linux de kernel reciente.

El mecanismo “trunkeado” se hace cargo de recalcular el RFC. En recepción, se eliminan esos 4 bytes y se envía a la VLAN que corresponda (VLAN ID), según la información que tengamos en la cabecera.

VTP

En equipos Cisco existe el protocolo VTP (VLAN Trunking Protocol) que permite crear dominios de VLANs, en los que varios switches comparten la información de las VLANs. Esto permite configurar un equipo y que el resto de equipos pertenecientes a este dominio queden configurados.

VMPS

Un VMPS (VLAN Management Policy Server) es un servidor que mapea direcciones MAC a VLANs. De esta forma, no tenemos que configurar el switch cada vez que conectamos un dispositivo, si no que cuando el dispositivo sea identificado por el switch, se le asignará automáticamente la VLAN que le corresponde.

Cuando un cliente VMPS (normalmente un switch) manda una consulta, a través de VQP (VLAN Query Protocol), el servidor VMPS responderá en función del mapeo y de si su modo de funcionamiento es seguro. De esta forma, si encuentra la dirección MAC y la VLAN no esta restringida a unos puertos del switch o el puerto al que esta conectado el dispositivo es correcto, enviará la VLAN a la que pertenece este dispositivo. Si no encuentra la MAC en su base de datos, según si existe una VLAN alternativa (denominada fallback VLAN) enviará esta y si no existe esta VLAN alternativa rechazará al dispositivo.

Tanto en este caso como en el caso de que el puerto al que esta conectado el dispositivo no este permitido, la respuesta de rechazo del dispositivo varía en función del modo de funcionamiento. De esta forma, esta respuesta será de denegación del acceso si el modo es abierto (open) y de desconexión del puerto si el modo es seguro (secure).

En el laboratorio se encuentra disponible el switch Cisco Catalyst 2950. Este switch no puede trabajar como servidor VMPS pero si como cliente.

La función de servidor puede realizarla un switch de mayores prestaciones o un PC en el que este corriendo un servidor VMPS.

Existen servidores VMPS de código abierto como OpenVMPS. Este sencillo servidor ofrece diferentes posibilidades para realizar el mapeo entre direcciones MAC y VLANs.

Una opción es a través de un archivo de configuración en el que se asigna el mapeo, además de políticas de puerto. Con estas políticas además de asignar a cada MAC su VLAN correspondiente, definimos la posibilidad o no de conectar

este dispositivo en cierto puerto del switch.

Otra opción es a través de un programa externo ligado a este servidor, que recibe la consulta de la MAC y devuelve la VLAN correspondiente. De esta forma podemos tener esta base de datos en un servidor central que por ejemplo trabajase con MySQL.

Existen otros servidores de código abierto como ICARUS VMPS que trabaja en JAVA o también existe un software de configuración de LANs y VLANs, FreeNAC que también realiza esta función aunque internamente utiliza el mismo servidor que OpenVMPS.

Continuar

Usted está en el sistema como Morató Osés Daniel (Salir)
Contacto: info@tlm.unavarra.es