Administración de Sistemas

1 - Aspectos Administrativos

Diciembre 2003

Guillermo Pérez Trabado

Dept. Arquitectura de Computadores

Universidad de Málaga

Planificación de la red

- Es necesaria la existencia de un responsable que defina la configuración y la mantenga: el Administrador de red.
- Analizar las necesidades presentes y las posibilidades de crecimiento de la red.
- Las decisiones en el diseño incluyen diversos aspectos:
  - Topología física: medios de transmisión, equipos activos.
  - Topología lógica: red plana o subredes.
  - Ubicación de los servidores (distribución del tráfico).
  - Tipos de direcciones usados, cortafuegos, proxys, enmascaramiento PAT y NAT.
  - Servicios de infraestructura: DNS, DHCP, Proxy-cache, estafetas de correo (SMTP, POP, IMAP), LDAP, etc.

Sobre el responsable

- Autoridad y competencias reconocidas oficialmente.
- Es muy recomendable la aprobación y publicación de unas normas de uso de la red donde se adviertan los derechos y deberes de los usuarios.
  - Evita usuarios manipulando configuraciones.
  - Reduce trabajos de mantenimiento por “imprevistos”.
- Establecer protocolos de resolución de problemas.
  - En organizaciones muy grandes, o subordinadas a otras, establece la cadena de contactos para resolver problemas.
  - En cada nivel de la jerarquía debe haber uno o más responsables con direcciones de email y números de teléfono conocidos por los administradores de los niveles adyacentes.
  - Evita la “redundancia” en la resolución de conflictos: no saltarse la jerarquía (excepto en emergencias). Esto incluye a los usuarios.

Análisis de las necesidades

- Utilización de la red: docencia, investigación, servicios de intranet , servicios de internet.
  - Número de computadores a conectar.
  - Crecimiento futuro.
  - Tráfico esperado.
  - Requerimientos de seguridad.
  - Tipos de sistemas operativos.

Topología física

- Medios de transmisión:
  - Pares trenzados clase 5 y clase 6 entre los puntos y los paneles de parcheo-elementos activos.
  - Fibras ópticas entre armarios con elementos activos.
  - También para salas con grandes servidores.
  - Sobredimensionar el número de cables aunque no se instalen las rosetas.
- Los elementos activos pueden ser reemplazables manteniendo los medios de transmisión si los medios cumplen unas características mínimas.

Topología lógica

- Se puede optar por una red plana o jerárquica a nivel MAC:
  - Plana: los paquetes de broadcast llegan a todos los nodos de la red. Si la topología física es jerárquica, esto se logra con bridges.
    - Ventajas: algunos servicios son más sencillos de configurar.
    - Inconvenientes: aumenta el tráfico total y la seguridad se ve comprometida (sniffers).
  - Los elementos activos actuales (ethernet) usan bridging inteligente. El tráfico solo se envía al puerto de destino incluso dentro de una subred.
  - Jerárquica: Existen zonas separadas de broadcast. La comunicación entre las mismas solo es posible mediante encaminamiento (routing).

Ubicación de los servidores

- Balance entre aspectos de seguridad y tráfico:
  - Por seguridad conviene ubicarlo en una sala segura (cerradura, refrigeración, SAI, mantenimiento).
  - Por eficiencia y seguridad conviene que esté cerca de las maquinas clientes (aulas, despachos). Evita que el tráfico atraviese el troncal de la red (backbone).
    - Las VLANs reducen, en parte, los problemas de seguridad de este caso.

Tipos de direcciones

- Direcciones privadas.
  - Son una solución para el crecimiento sin restricciones del número de máquina.
  - No pueden salir de la intranet de la organización.
  - No permiten el uso de ICMP, UDP ni TCP desde/hacia otra máquina fuera de la organización.
  - Reducen riesgos de seguridad, pero limitan la funcionalidad.
  - No sirven para servidores públicos.
  - Requiere el uso de un router a la salida de la subred y de un proxy para poder usar servicios de Web y FTP.
  - Se puede usar enmascaramiento para resolver las limitaciones para otros protocolos y simplificar la configuración (NAT, PAT).

Enmascaramiento

- Requiere un cortafuegos. Hay dos técnicas básicas:
  - PAT: El firewall suplanta la dirección de la máquina interna y el puerto TCP/UDP con su propia dirección pública y un puerto libre.
    - Limitación: Para “servicios bien conocidos” solo puede haber un servidor en la intranet (FTP, HTTP, SMTP,...).
  - NAT: El firewall dispone de una colección de direcciones para suplantar la dirección de la máquina interna. El puerto no es traducido.
    - Limitación: Puede haber menos direcciones que máquinas intentando conectar fuera. La dirección usada puede cambiar entre dos conexiones consecutivas.
    - Permite asignar direcciones externas fijas a servidores internos que deben ser encontrados desde fuera.

Servicios de infraestructura

- Hay un conjunto de servicios que ofrece y gestiona el administrador de la red:
  - DNS: resolución de direcciones.
  - DHCP: asignación dinámica de direcciones.
  - Router: salida de la subred.
  - Proxy-Cache: salida a internet.
  - Correo: SMTP, POP, IMAP
  - NIS: nombres de usuarios en un cluster UNIX.
  - NNTP: servidor de tiempo.

Controlando la configuración

- La configuración errónea de un sistema en una red puede afectar a todos los sistemas del conjunto:
  - Problemas de funcionamiento básico.
  - Alteraciones en los niveles de tráfico.
  - Debilitamiento en la seguridad de la intranet.

Problemas de funcionamiento básico

- Direcciones duplicadas.
- Máscaras de red erróneas.
- Routing mal configurado.
- Broadcast incorrecto.

Problemas de tráfico

- Servicios mal configurados
  - Exceso de tramas de broadcast.
  - Routing ineficiente.
  - Servicios “ilegales” (emule, edonkey, etc).
  - Servidores mal ubicados.
- Problemas crónicos
  - Subredes con usos que superan las previsiones iniciales durante el diseño.

Compromisos en la seguridad

- La cadena siempre se rompe por el eslabón más débil:
  - Virus de windows: ¿Es Windows propiamente un virus?
  - Servicios habilitados con vulnerabilidades.
  - Servicios sin autenticación, cuentas sin password.
  - Ataques DoS (Denial of Service).
- ¡Importancia de las actualizaciones!

Configurando un sistema aislado

- Pasos a seguir:
  1. Desconectar la máquina de la red.
  2. Contactar con el administrador de la red si no tenemos esa competencia.
  3. Indicar el punto donde se va a conectar (suelen estar etiquetados) y qué pretendemos conectar.
     - Puede estar desactivado.
     - Puede estar conectado a una VLAN distinta a la que creemos.
     - El administrador suele llevar un registro de qué está conectado en cada punto.
     - Obtener los parámetros del punto: 10BaseT, 10/100BaseT, ¿autonegociado?, ¿half/full-duplex?

Configurando un sistema aislado

4. Obtener parametros IP: dirección IP, máscara, dirección de broadcast, dirección del router, proxy autorizado, servidores DNS, servidores WINs, servidor NNTP.
5. Si el nombre no existe en DNS elegir un nombre único y pedir su alta en el servidor.
6. Instalar el sistema operativo y configurarlo.
7. Deshabilitar todos los servicios que no se necesiten o se desconozcan.
8. Verificar que todas las cuentas tienen password.

Configurando un sistema aislado

9. Instalar actualizaciones del sistema, desde CD o usando una dirección privada.
10. Instalar antivirus.
11. Instalar y configurar cortafuegos personales: ZoneAlarm (Windows), IPChains (Linux).
12. Conectar a la red.

Configurando una subred

- Si el número de máquinas a administrar es suficientemente elevado puede ser necesario delegar la responsabilidad de gestión en un administrador.
- Implica la asignación de una serie de recursos por adelantado que serán gestionados de forma autónoma:
  - Rango de direcciones.
  - Dominio DNS propio.
  - Servidores independientes: DNS, correo, DHCP, proxy, NIS, NNTP.

Configurando una subred

- Pasos a seguir:
  1. Contactar con la administración de la que depende la futura subred y analizar el proyecto.
  2. Obtener un nombre de dominio (opcional).
  3. Obtener uno o varios rangos de direcciones IP.
  4. Establecer una o varias VLANs con la lista de puntos de red de la subred.
  5. Analizar la necesidad de usar un cortafuegos para salir de la VLAN.
  6. Si se no se tiene un servidor DNS propio se puede configurar un servidor Cache de DNS propio.
  7. Si hay portátiles o máquinas que cambian con frecuencia (averías en laboratorios), configurar un servidor DHCP.

Configurando una subred

8. Si vamos a tener un servidor de correo, debe estar declarado con una entrada MX en DNS.
9. Configurar un servidor de tiempo NNTP dependiente del servidor que le corresponde.
10. Configurar un servidor de información de usuarios: NIS (UNIX), un Dominio de Windows o un grupo de trabajo.
11. Definir una configuración de seguridad:
    - Qué máquinas tienen activados qué servicios públicos: WEB, FTP, NFS, SAMBA, etc.
    - Eliminar estos servicios en el resto de máquinas.
    - Restringir el acceso a toda máquina que no pertenezca al grupo para todos los servicios restantes.
    - Dejar una sola puerta de acceso desde el exterior en una sola máquina. Por ejemplo SSH.