

SNMP (Simple Network Management Protocol)

Introducción

Como su nombre lo dice, el Protocolo Simple de Administración de Redes, muestra una manera de administrar y supervisar las redes de cómputo para identificar y resolver problemas, así como para planear su crecimiento, esto a través de una relación cliente/servidor entre el gestor de red y los elementos gestionados. SNMP es un protocolo que pertenece a la familia TCP/IP y su funcionamiento es sencillo aunque su implementación bastante compleja.

Está cubierto por un gran número de RFC's (Request For Comments), entre ellos

Versión 1	1157, 1215
Versión 2	del 1441 al 1452
Versión 3	del 2271 al 2275 y del 2570 al 2575

El esquema es sencillo, sin embargo su complejidad se incrementa a la hora de definir el formato de las variables. Maneja una base de datos de información gestionable que contiene, organizados de forma jerárquica, valores de control. Esta se llama MIB, es una sola aunque existen múltiples extensiones a ésta, además de está descrita en ASN.1 para facilitar su transporte transparente por la capa de red.

SNMP presenta ciertas ventajas que pueden ser muy útiles y deberían ser tomadas en cuenta en contra de la difícil implementación que presenta.

- Es popular, puesto que casi todo elemento de red lo maneja.
- Flexibilidad, debido a que se puede adaptar a las necesidades de gestión.
- Extensible puesto que puede aprender nuevos MIB's de forma automática
- Simple, en la forma de pregunta-respuesta que maneja, para obtener o actualizar los valores de los objetos que monitorea.

Además, se presentan algunos ejemplos de lo que se puede realizar con este protocolo:

- Programar un interfaz para tomar medidas en base a la consultas sobre las características de un elemento de red.
- Recibir alertas y tratarlas como sea necesario.
- Hacer que el agente ejecute comandos con la función exec como toma de acciones dentro del sistema.
- Hacer que el agente controle la carga de la máquina con el parámetro load.
- Configurar el agente para enviar alertas a otros agentes
- Modificar las tablas de rutado de un router.
- Conocer las estadísticas de funcionamiento de un servidor.
- Desconectar una estación de trabajo de la red.
- Ver los paquetes que circulan por una subred.
- Conocer la temperatura de funcionamiento de un concentrador.

SNMP cuenta con 4 componentes principales:

1. Sistema de Administración de Redes (SAR), es un software que ejecuta aplicaciones de administración y monitoreo sobre los elementos administrados.
2. Elementos administrados. Los elementos administrados son cualquier nodo de la red que contiene un agente SNMP, son elementos como: servidores, ruteadores, impresoras, etc., los cuales recopilan información administrable para el SAR, tal que es accesada por medio del protocolo SNMP.
3. Un agente SNMP es un software que reside en el elemento administrado, el cual toma la información de administración recopilada por este elemento y la traduce para que sea compatible con el SAR.
4. El protocolo SNMP es el protocolo por medio del cual el elemento administrado proporciona la información de administración al SAR

SNMP en linux

En la mayoría de los sistemas Linux se llamaba ucd-snmp a distribuciones previas de SNMP, actualmente se conoce como net-snmp e incluye soporte para todas las versiones de la uno a la tres de SNMP.

snmpd es un agente que permanece escuchando en el puerto 161 (UDP), esperando recibir peticiones, cuando le llega una solicitud la procesa y devuelve la información.

snmptrapd es un agente que procesa las alertas de otros agentes, permanece escuchando el puerto 162 (UDP), y cuando recibe una alerta procede a guardarla en el registro syslog

Los agentes de net-snmp incluyen una serie de extensiones:

- Información general del sistema
- Conexiones TCP / UDP / IP / SNMP abiertas y estado
- Discos duros
- Procesos y carga del procesador

Los agentes pueden ser por ejemplo:

- Ordenadores conectados a la red
- Servidores
- Bridges
- Routers
- Concentradores
- Hubs
- Impresoras de red

Visión rápida sobre la instalación

Una vez descargados y descomprimidos los paquetes TAR/GZ, se debe compilar el código con las instrucciones abajo descritas.

```
./configure
make all
make install
```

Otra forma sencilla es instalar los paquetes ucd-snmp-xxx.i386.rpm y ucd-snmp-xxx.i386.rpm de la siguiente forma:

```
rpm --nodeps -i ucd-snmp-xxx.i386.rpm
rpm -i ucd-snmp-xxx.i386.rpm
```

El siguiente paso es configurar el archivo /etc/snmp/snmpd.conf. El manual snmpd_config describe el funcionamiento general de los ficheros pero en general se debe definir una relación entre comunidades y modelos de seguridad en el agente SNMP, es decir, una relación entre modelos de seguridad y grupos, se definen también vistas o zonas del árbol de la MIB, y por último, se indica el acceso permitido de los grupos a las vistas.

Configurar el demonio SNMP
/etc/snmp/snmpd.conf

Iniciar el servicio SNMP con:
/etc/rc.d/init.d/snmpd start ó
service snmpd start (solo root)

Probamos que el servicio funciona como sigue:
snmpwalk localhost [comunidad] [MIB]

Ejemplo:
snmpwalk localhost secreto system
snmpwalk localhost secreto interfaces

Arquitectura de SNMP

Para hacer más eficiente la administración de red, se dividen las actividades en dos partes:

- a) Monitoreo o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- b) Control o proceso de cambiar el comportamiento de la red en tiempo real, ajustando parámetros, mientras la red está en operación para mejorar el funcionamiento y reparar fallas.

El manejo de una red TCP/IP consiste de una estación manejador de red (network management stations) o *managers*, comunicándose con los elementos de la red. Estos elementos de la red pueden ser cualquier cosa que corre bajo TCP/IP (host, ruteadores, terminales X, servidores, impresoras, etc.). El software en el elemento de red que realiza el manejo del software es llamado *agente*. Las estaciones de manejo son normalmente estaciones de trabajo que grafican los elementos monitoreados.

La comunicación puede ser de dos tipos:

- El manager preguntando al agente por un valor específico.
- El agente diciendo al manager que algo importante a ocurrido.

Sin embargo, es posible también que el manager modifique las variables en el agente.

El manejo de una red TCP/IP se basa en tres partes:

1. *Management Information Base* (MIB) que especifica que variables mantienen los elementos de red.
2. *Structure of Management Information* (SMI). Estructuras y un esquema que identifica las características de las variables en el MIB.
3. *Simple Network Protocol* (SNMP). El protocolo entre el manager y el elemento que detalla el formato de los paquetes intercambiados.

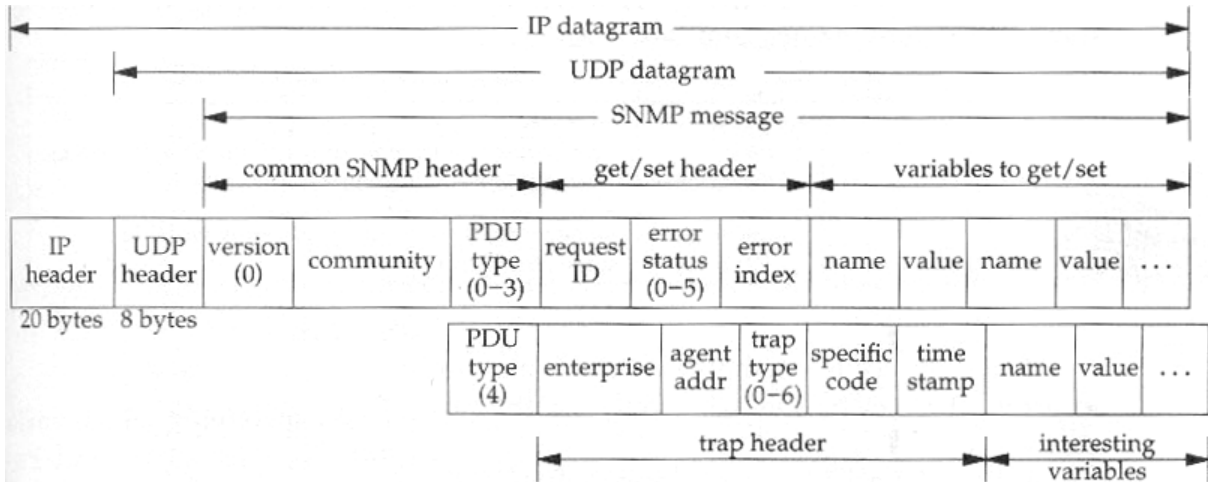
El protocolo SNMP tiene dos metas principales: la primera es minimizar la cantidad de mensajes intercambiados entre las entidades de red con el contenido de la información solicitada para la administración de las redes, es por esto que surgen los mensajes "Trap". Los mensajes trap son mensajes espontáneos que un dispositivo de red envía al administrador únicamente cuando sucede algún evento ya especificado, es decir, cuando detecta una condición predeterminada. La segunda meta es la simplicidad, ya que SNMP utiliza únicamente un subconjunto de reglas del código básico ASN.1 para definir la manera en que la información será estructurada.

SNMP define solo 5 tipos de mensaje que son intercambiados entre el manager y el agente.

- *get-request* pide el valor de una o más variables.
- *get-next-request* pide el valor de una o más variables especificadas con anterioridad.
- *set-request* establece el valor de una o más variables.
- *get-response* es la respuesta del agente al manager de los operadores anteriores.
- *trap* notifica al manager cuando algo sucedió.

Los primeros tres mensajes son enviados por el manager hacia el agente y los últimos dos por el agente hacia el manager. Esto se realiza por medio del protocolo UDP, lo cual no garantiza que lleguen los mensajes y por lo tanto deberían establecerse *timeouts* o tiempos de espera para retransmitir.

El manager envía su mensaje por el puerto 161 y el agente por el puerto 162. Se basa en los siguientes formatos, pero no se especifica el tamaño en bytes, debido a que se basa en una codificación ASN.1 y BER.



La *versión* es el número de versión real menos uno.

El *tipo de PDU* puede ser:

Tipo	Nombre
0	get-request
1	get-next-request
2	set-request
3	get-response
4	trap

El *community* es una cadena de carácter con un password entre el manager y el agente.

El *request-ID* lo modifica el manager si se ocupan los tres primeros tipos de PDU y el agente regresa su respuesta por el get-response.

El *error-status* es un número entero que especifica un error como sigue:

error-status	Nombre	Descripción
0	noError	Todo esta bien.
1	tooBig	El agente no podría responder en un mensaje simple SNMP.
2	noSuchName	Operación especificada con una variable inexistente.
3	badValue	Una operación especificada con un valor o sintaxis inválido.
4	readOnly	Manager trata de modificar una variable de solo lectura.
5	genErr	Algún otro error

El *error-index* es un número entero, especificado por el agente, para identificar a la variable con error, solamente si el error-status es 2, 3 o 4.

get request

El número de variables máximo que se pueden procesar es limitado por el tamaño máximo que puede manejar el agente y el manager. Sin embargo, deben ser capaces de manejar PDU's mayores a 484 bytes.

Si ocurre algún problema al solicitar alguna variable en la lista de la PDU, el mensaje get-request falla y ninguna información es regresada.

get next request

La respuesta que recibe es un PDU del tipo get-response, y su objetivo está recorrer fila por fila y en orden lexicográfico, dentro de la tabla de variables que tiene el SNMP para regresar su valor.

Las variables son apropiadas para puentes, routers y hosts. Por ejemplo, en un par de routers, las variables pueden variar debido a que en una interfaz se conectan una red Ethernet y una FDDI, mientras que en la otra pueden estar conectadas una red Token-Ring y T1. Por eso es necesario manejar los nodos de manera correcta.

La primer forma consiste en crear un una base de datos maestra manualmente, para el manejo de la estación, donde se puedan determinar:

- El tipo de nodo (puente, router o host).
- Las categorías de las variables MIB soportadas en el nodo.

Esta base de datos se mantiene manualmente, borrando y agregando entradas en varios nodos. La segunda forma es implementar una aplicación que descubra los nodos en una red y después pregunte que son y qué variables soporta. Esto se puede hacer al preguntar con get-next-request, continuamente, hasta que genere un error por no existir mas variables.

Trap

Son mensajes puestos al alcance del agente para reportar condiciones serias del manejo de la estación y deben ser usadas cuidadosamente.

El campo *Enterprise* contiene un OBJECT IDENTIFIER que, normalmente, lo define el administrador. Puede contener un identificador para una rama del MIB que define una tecnología para la cual, el trap esta definido o puede tener un identificador del cuerpo administrativo del trap.

Network Address contiene la dirección IP del host que envió el trap.

Generic Trap identifica el tipo de trap enviado:

tipo trap	Nombre	Descripción
0	coldStart	El agente está inicializándose a sí mismo.
1	warmStart	El agente esta reinicializándose a sí mismo.
2	linkDown	Una interfaz ha cambiado a un estado inactivo. La primer variable en el mensaje identifica la interfaz.
3	linkUp	Una interfaz ha cambiado a un estado activo. La primer variable en el mensaje identifica la interfaz.
4	authenticationFailure	Un mensaje fue recibido de un manager con <i>community</i> erróneo.
5	egpNeighborLoss	Cuando un nodo EGP se ha caído. La primer variable in el mensaje, contiene la dirección IP del nodo.
6	enterpriseSpecific	Ver el campo de código específico para más información

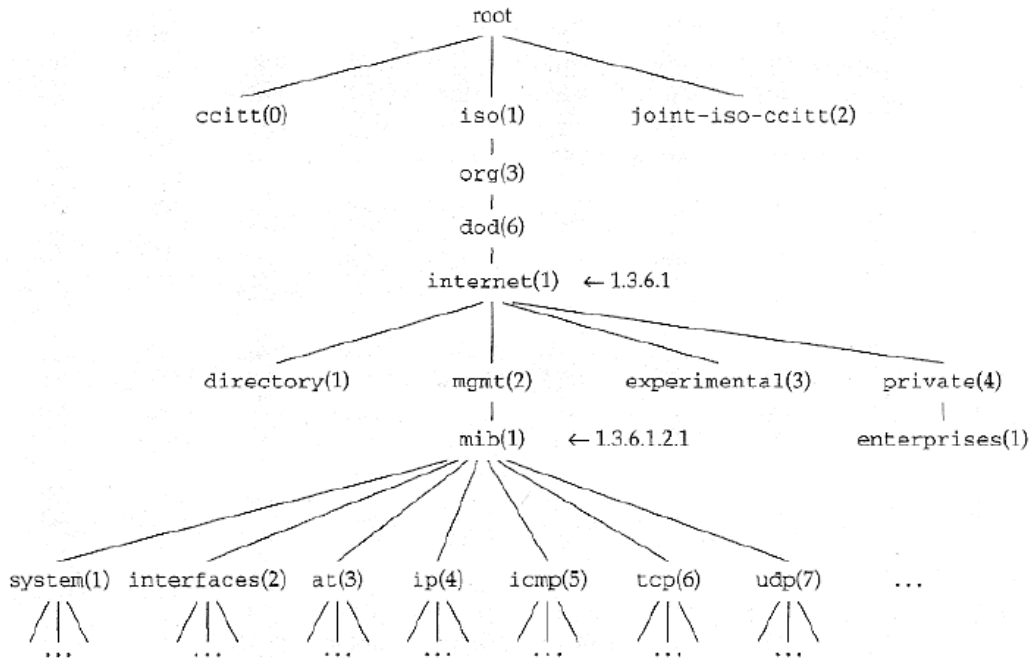
Specific Trap es usado para identificar el trap al que se refiere el administrador, si se utiliza un trap del tipo 6 ó *enterpriseSpecific*.

Timestamp reporta un tiempo transcurrido entre la inicialización de la entidad y la generación del trap.

El resto de variables que son incluidas en el trap vienen en pares como en get-request, lo cual permite identificar donde a ocurrido el suceso reportado.

Object Identifier

Es un tipo de dato que se presenta en la forma de una secuencia de enteros separados por puntos decimales. Estos enteros dibujan una estructura de un árbol con una raíz en la parte mas alta, llamada root. Como se ve en la figura, el árbol describe la ruta a seguir para identificar donde inicia las variables MIB (1.3.6.1.2.1 ó iso.org.dod.intenet.mgmt.mib).



Se puede observar también que existe otra rama denominada iso.org.dod.internet.private.enterprises (1.3.6.1.4.1), ésta es la que identifica la localización de la MIB privada o que cada empresa implementará para sus propios intereses.

MIB (Management Information Base)

La MIB es una base de datos de información que mantiene el agente y que un manager puede consultar o definir sus valores. Como se muestra en la figura anterior, la MIB se divide en grupos como system, interfaces, at (address translation ó traducción de direcciones), ip y otros.

La MIB - I (ó versión 1) define 126 objetos de administración que son divididos en los 8 grupos siguientes:

- | | |
|---|--------------|
| 1. Grupo de Sistemas | (system) |
| 2. Grupo de interfaces | (interfaces) |
| 3. Grupo de Address Translation | (at) |
| 4. Grupo de Internet Protocol | (ip) |
| 5. Grupo de Internet Control Message Protocol | (icmp) |
| 6. Grupo de Transmisión Control Protocol | (tcp) |
| 7. Grupo de Unit Datagram Protocol | (udp) |
| 8. Grupo de External Gateway Protocol | (egp) |

Sin embargo, el MIB - I, no incluye información de administración para aplicaciones como TELNET, FTP y SMTP debido a que es dificultoso para las compañías fabricantes instrumentar aplicaciones de este tipo para el MIB.

El MIB - II pretende extender los datos de administración de red empleados en redes Ethernet y redes globales usando elementos orientados a múltiples medios de administración en redes LAN y WAN. MIB - II agrega dos grupos más a los ocho que ya están en la MIB - I.

El RFC 1156, llamado Base de Información Administrable para Redes en Internet basadas en TCP/IP, es un documento donde se define la primera versión de la Base de Información Administrable (MIB)

Los características de los grupos MIB son los siguientes:

Grupo	Descripción
-------	-------------

System	Se usa para registrar información del sistema en el cual corre la familia de protocolos, por ejemplo: <ol style="list-style-type: none"> 1. Compañía fabricante del sistema 2. Revisión del software 3. Tiempo que el sistema ha estado operando
Interfaces	Este grupo registra información genérica acerca de cada interfaz de red, por ejemplo el número de mensajes erróneos en la entrada y en la salida, número de paquetes transmitidos y recibidos, número de paquetes de broadcast enviados, entre otros. Solo consiste de una variable simple que identifica dicha interfaz de red (ifNumber) y una tabla con 22 columnas que definen las características para cada interfaz.
at	Aunque fue deprecado por la MIB-II, este grupo define una tabla con tres columnas que identifican el número de interfaz, la dirección física y la dirección IP de las máquinas de una red.
Ip	Este grupo almacena información propia de la capa IP como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control que permite que aplicaciones remotas puedan ajustar el TTL de omisión de IP y manipular las tablas de ruteo de IP. Todo esto se almacena en varias variables y tres tablas: Tabla de direcciones IP, Tabla de ruteo IP y Tabla de traducción de direcciones IP
Icmp	Consiste de cuatro contadores generales (El total de mensajes ICMP de entrada y salida, y el número de mensajes ICMP de entrada y salida con error) y 22 contadores para los diferentes tipos de mensajes ICMP (11 contadores de entrada y 11 contadores de salida).
Tcp	Este grupo incluye información propia del protocolo TCP, por ejemplo estadísticas del número de segmentos transmitidos y recibidos. Información acerca de conexiones activas como dirección IP, puerto, estado actual, es decir, los estados de transición del protocolo en general.
Udp	Contiene pocas variables y una tabla simple, que se utiliza para mostrar los detalles de la identificación de instancias y el ordenamiento lexicográfico.
Egp	En este grupo se requieren sistemas (ruteadores), que soporten EGP.
Snmp	Este grupo incluye estadísticas sobre tráfico de red SNMP, por ejemplo: <ul style="list-style-type: none"> • Número de mensajes entregados al módulo TCP local. • Estadísticas de errores encontrados en mensajes de entrada • Número total de mensajes SNMP de salida • Número de mensajes entregados de cada tipo.
transmision	Este grupo soporta múltiples tipos de medios de comunicación como cable coaxial, cable UTP, cable de fibra óptica y sistemas T1 / E1.

La identificación de instancias en las variables simples es por medio de una referencia, al agregar un ".0" a la variable del object identifier. Por ejemplo, para el nombre textual iso.org.dod.internet.mgmt.mib.udp.udpInDatagrams.0 su object identifier es: 1.3.4.1.2.1.7.1.0.

La identificación de instancias en tablas de entrada es mas detallada, puesto que uno o mas indices son especificados en el MIB para cada tabla. Por ejemplo, para la tabla del grupo UDP, la MIB define un índice como la combinación de dos variables, udpLocalAddress que es la dirección IP y udpLocalPort que es un entero que define el puerto de comunicación. Suponiendo que en la tabal existen tres renglones, el primero es para la dirección 10.0.0.1 en el puerto 67, el segundo para la dirección 10.0.0.1 en el puerto 161 y el tercero en la dirección 10.0.0.1 en el puerto 520, lo cual implica que el sistema está esperando recibir datagramas UDP de alguna interfaz por los puertos 67 (BOOTP server), 161 (SNMP) y 520 (RIP).

udpLocalAddress	udpLocalPort
0.0.0.0	67
0.0.0.0	161
0.0.0.0	520

Para poder hacer referencia a estos datos, la MIB se basa en un ordenamiento lexicográfico por medio de sus object identifiers, esto significa que los datos que mencionamos en la tabla anterior son organizados y accesados por el operador get-next de la siguiente forma.

Su organización:

Columna	Object identifier	Nombre abreviado	Valor
1	1.3.6.1.2.1.7.5.1.1.0.0.0.0.67	udpLocalAddress.0.0.0.0.67	0.0.0.0 0.0.0.0 0.0.0.0
	1.3.6.1.2.1.7.5.1.1.0.0.0.0.161	udpLocalAddress.0.0.0.0.161	
	1.3.6.1.2.1.7.5.1.1.0.0.0.0.520	udpLocalAddress.0.0.0.0.520	
2	1.3.6.1.2.1.7.5.1.2.0.0.0.0.67	udpLocalPort.0.0.0.0.67	67 161 520
	1.3.6.1.2.1.7.5.1.2.0.0.0.0.161	udpLocalPort.0.0.0.0.161	
	1.3.6.1.2.1.7.5.1.2.0.0.0.0.520	udpLocalPort.0.0.0.0.520	

Su acceso:

udpLocalAddress	udpLocalPort
0.0.0.0	67
0.0.0.0	161
0.0.0.0	520

Comandos de SNMP en la distribución Linux

arpnmp

Guarda pares de direcciones Ethernet/IP. Se almacena la actividad en syslog y envía un reporte de los cambios por e-mail.

snmpbulkget

Se comunica con un elemento de red usando SNMP BULK requests.

snmpbulkwalk

Se comunica con un elemento de red usando SNMP BULK requests.

snmpd

Es un agente que responde a paquetes SNMP request. Monitorea redes.

snmpdelta

Establece un proceso de monitorización sobre una o más variables del agente de manera que se recupere el valor de estas variables en ciertos periodos de tiempo definidos.

snmpget

Se comunica con un elemento de la red, usando SNMP GET requests.

snmpgetnext

Se comunica con un elemento de la red usando SNMP GET NEXT requests.

snmpnetstat

Permite obtener un listado de los canales de comunicación abiertos en una máquina, es decir, el estado de la red.

snmpset

Se comunica con un elemento de la red usando SNMP SET requests.

snmpstatus

Recupera información sobre el estado de un host en una red.

snmptable

Muestra las tablas de SNMP después de recuperar el valor de una variable.

snmptest

Es una herramienta de prueba del agente que permite recuperar el valor de las variables que contiene a través de una interfaz de comandos.

snmptranslate

Traduce un ID de un objeto SNMP a una cadena de texto con el nombre del objeto.

snmptrap

Envía un trap de SNMP al manager.

snmptrapd

Recibe y guarda en archivos log, los mensajes trap.

snmpusm

Administra usuarios SNMP version 3 en un elemento de red remoto.

snmpwalk

Se comunica

Realizó

Oswaldo Herrera

México D.F.

waldosoc@yahoo.com.mx

Aydee Juárez

México D.F.

apafu3007@yahoo.com.mx

Bibliografía

- ✓ W Richard Stevens, "TCP/IP Illustrated, The Protocols", Volumen 1, Addison Wesley, 1994
- ✓ Dr. Sidnie Feit, "SNMP, A guide to network management", McGraw Hill, 1995

Bibliografía recomendada por otros autores

Corner, "Internetworking with TCP/IP: Principles, protocols and architecture"

Corner, "Internetworking with TCP/IP: Design, implementation and internals"

Corner, "Internetworking with TCP/IP: Client/server programming and applications"

Pisticello, "Open Systems networking: OSI & TCP/IP"