Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

TEMA:

Implementación de una herramienta de administración y monitoreo de servidores basada en Windows que permita la gestión de la red de forma remota a través de una conexión vpn con fines académicos para los estudiantes de la carrera Técnico en Ingeniería de Redes

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Darvi Alan Pérez Ascencio

Ricardo Ernesto Leiva

Roberto Antonio Suárez

PARA OPTAR AL GRADO DE:

Técnico en Ingeniería de Redes Computacionales

SEPTIEMBRE DE 2008

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

AUTORIDADES

LIC. JOSÉ MAURICIO LOUCEL
RECTOR

ING. NELSON ZÁRATE SÁNCHEZ
VICERRECTOR ACADÉMICO

ING. LORENA DUQUE DE RODRÍGUEZ
DECANO

JURADO EXAMINADOR

LIC. CARLOS ALFREDO MORALES GÓMEZ
PRESIDENTE

ING. JULIO CESAR MENÉNDEZ RODRÍGUEZ
PRIMER VOCAL

LIC.WALTER MAURICIO NAVARRETE HERNÁNDEZ
SEGUNDO VOCAL

SEPTIEMBRE, 2008

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AGRADECIMIENTOS

- Agradezco a Dios por darme la oportunidad de terminar este proyecto y por darme la fortaleza y sabiduría de seguir adelante por haber guiado mis pasos, por darme la salud y permitirme lograr realizar mis sueños y mis metas de finalizar mi carrera.

- A mis padres, por la oportunidad de existir, por su sacrificio, por su ejemplo de superación incansable, por su comprensión y confianza, por su amor y amistad incondicional, porque sin su apoyo no hubiera sido posible la culminación de mi carrera profesional.

- Agradezco el apoyo de mi asesor y sus colegas jurados, a mis compañeros de clases y amigos que estuvieron conmigo, a mis maestros y profesores que me dieron su apoyo en especial al Lic. Walter Navarrete que me guío durante este proceso y a mis compañeros de trabajo Darvi Pérez y Roberto Suárez por su apoyo en todo momento y a todas aquellas personas que de una u otra forma estuvieron involucradas en este trabajo.

- A la Universidad Tecnológica de El salvador por darme la formación profesional en Técnico en Ingeniería en Redes Computacionales.

Ricardo Ernesto Leiva

AGRADECIMIENTOS

- Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.
- A mis padres, por el apoyo que me brindaron, por la formación, por fomentar en mi el deseo de saber, de conocer lo novedoso y abrirme las puertas al mundo ante mi curiosidad insaciable.
- A nuestro asesor, por la orientación que nos brindo durante el proceso de graduación.
- A la Facultad de Ciencia y Tecnología, por el soporte institucional dado para la realización de este trabajo.
- Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de esta tesis.

Darvi Alan Pérez Ascencio

AGRADECIMIENTOS

- Gracias infinitas a Dios que siempre ha estado conmigo y me ha dado la sabiduría y el entendimiento necesario en todo este tiempo, por darme la fortaleza suficiente para poder vencer los obstáculos que se me han presentado y por todas las bendiciones que me ha dado, que entre las más grandes está la de permitirme alcanzar este logro.

- A mis padres, Roberto Antonio y Ana Teresa, por haber logrado con su esfuerzo darme la oportunidad de estudiar, por apoyarme en todo momento, brindarme su confianza (en la mayoría de los casos).

- A mis hermanos, que a pesar de las dificultades siempre han estado ahí y por apoyarme también(cada cual a su modo).

- A mi hijo por cambiarme la vida y llenarla de amor, a mis sobrinos por dar alegrías mas que cualquier otra cosa.

- A mis tíos, abuela, y a ti Maria que siempre creíste y que han creído en mí dándome ánimos para poder seguir adelante, por darme su amor, confianza e inculcarme valores positivos para ser una persona de bien (en la manera de lo posible).

- A mis amig@s, compadres y herman@s de toda una vida de desvelos de estudio y las que son objeto del mismo también gracias por el apoyo incondicional.

- A ti Norma por estar a mi lado por apoyarme y aguantarme en esta etapa de mi vida y a la vez por ser inspiración de la misma.

- A todos los que Dios ha permitido ponerlos en mi camino poniendo esas pecas que dan color y que de alguna manera han dado luz a mi vida brindándome consejos, su tiempo, momentos inolvidables, su cariño, jalones de aire y muchas grandes experiencias que me han hecho crecer como persona.

Roberto Antonio Suárez Hernández

ÍNDICE DEL CONTENIDO

CONTENIDO PAGINA

INTRODUCCIÓN

La necesidad de contar con una red empresarial segura, funcional y de fácil manejo, se vuelve cada día mas indispensable, debido a que la tecnología se encuentra en constante crecimiento, hoy en día a evolucionado de tal manera que es imposible realizar las labores diarias sin tener que recurrir al uso de una computadora ya sea para la utilización de un sistema de aplicaciones o simplemente para revisar el correo electrónico.

Precisamente debido a estas exigencias, el propósito de este material es orientado a la implementación de un sistema de gestión remota de redes, que permita monitorear y administrar equipos terminales y servidores de manera centralizada.

Todo esto se puede lograr con una o varias herramientas que se utilizan para la realización de este tipo de tareas, la exigencia de mantener muy bien administrado un sistema es esencial y es por ello que muchas veces se debe realizar este tipo de gestiones a horas no laborales o cuando se es casi imposible poseer físicamente el equipo, lo cual por medio de una red virtual privada se podrá optimizar el uso de las herramientas de monitoreo.

En el desarrollo del presente trabajo, se realizará un proceso de investigación de varias herramientas que permitan la gestión y control de redes de una forma segura y remota, para facilitar la labor administrativa de los equipos de red como servidores críticos de las empresas. De estas herramientas se estará

recomendando la más factible y que cumpla con los requisitos que posteriormente se clasificarán como críticos para la selección del producto.

CAPITULO I

1.GENERALIDADES DEL PROYECTO

1.1 SITUACIÓN PROBLEMÁTICA

Dentro de la carrera Técnico en Ingeniería de Redes de la Universidad Tecnológica no se cuenta con una herramienta que permita a los alumnos tener un panorama más claro sobre lo que es la administración de redes y servidores de forma centralizada y remota. Es por eso que este proyecto de investigación tiene como objetivo principal el investigar un conjunto de productos disponibles en el mercado, la selección y recomendación de un producto que sea factible de instalar y les permita a los estudiantes que puedan tener este tipo de experiencia dentro del desarrollo de sus carreras y de esa manera poder familiarizarse con este tipo de tecnología.

1.2 ENUNCIADO DEL PROBLEMA

¿Como logrará la Universidad Tecnológica brindar a los futuros Técnicos en Ingeniería de Redes una herramienta que les facilite el monitoreo y la gestión remota de un entorno de red de manera simple y centralizada?

1.3 JUSTIFICACIÓN DEL PROYECTO

El contar con una Herramienta de monitoreo y gestión de redes servirá de apoyo para las practicas de laboratorio de los alumnos de la carrera Técnico en Ingeniería de Redes, poniendo a disposición de los alumnos y docentes dicha herramienta para la gestión de redes de forma remota y centralizada.

Es importante este trabajo porque se pretende mejorar los servicios informáticos de la carrera Técnico en Ingeniería de Redes; pues esta presenta falta de materiales y recursos para la realización de prácticas. Este tipo de actividades para dicho técnico es uno de los elementos fundamentales de esta, ya que permite que los alumnos logren poner en desarrollo todo el material teórico visto en las asignaturas y de esa manera prepararlos para la realidad que se ve día a día en el área de redes computacionales.

1.4 OBJETIVOS

OBJETIVO GENERAL

Analizar diferentes herramientas para la administración y gestión de redes que permita de una forma efectiva y segura, la fácil administración de los recursos en la red.

OBJETIVOS ESPECÍFICOS

- Instalar la herramienta que será propuesta como la mejor alternativa

para administrar redes de forma remota.

- Desarrollar una guía para implementar dicha herramienta que permita administrar una red de forma centralizada.
- Proponer una alternativa de conectividad remota para poder administrar a través de una herramienta los servidores de una red local.

1.5 ALCANCES

- Controlar y gestionar de manera remota mediante una herramienta de control y de administración de redes de forma sencilla, fácil, y funcional desde una ubicación centralizada.
- Elaborar un manual de instalación y configuración para la utilización de la aplicación Solarwinds.
- Implementar una alternativa de conectividad que sea segura y de fácil uso para poder administrar remotamente la red de la empresa.

1.6 DELIMITACIONES

GEOGRÁFICA:

La implementación del sistema de gestión remota se implementará en los Laboratorios de la Facultad de Informática y Ciencias Aplicadas de la

Universidad Tecnológica de El Salvador.

TEMPORAL:

Este proyecto se realizará entre el periodo de febrero a junio del año 2008, para tal periodo de tiempo el proyecto se entregará en funcionamiento.

ORGANIZACIONAL:

El desarrollo de este proyecto será de beneficio para la carrera de Técnico en Ingeniería de Redes ya que este proyecto permitirá a los alumnos disponer de herramientas de software para crear prácticas virtuales dentro de los Laboratorios de la Universidad.

ESPECIFICA:

La implementación de este proyecto incluye una Herramienta de control y gestión de redes, además cuenta con una VPN basada en software libre la cual se implementará de manera virtual, ya que implementar un servidor con características robustas, es un recurso que no está a disposición para este proyecto.

1.7 ESTUDIO DE FACTIBILIDAD

TÉCNICA:

La realización de este proyecto tiene factibilidad técnica ya que la Universidad Tecnológica de El Salvador cuenta con los recursos necesarios

dentro de sus laboratorios, para su realización, tomando en cuenta que se implementará dentro de estos, para que los estudiantes de la carrera Técnico en Ingeniería de Redes puedan efectuar las practicas asociadas a la administración de redes.

ECONÓMICA:

Debido a que este proyecto está basado en una plataforma de licenciamiento libre no es necesario invertir económicamente con respecto al software a utilizar, sin embargo, si habría que realizar una inversión económica para la compra de la herramienta de monitoreo para la cual se presentará una tabla comparativa para evaluar la mejor selección.

OPERATIVA:

Dentro de la parte operativa será necesario realizar una inducción por medio de manuales y guías, para que los docentes y técnicos de centros de cómputo tengan conocimiento sobre el uso de la herramienta y de esa manera poder realizar las prácticas de forma eficiente, ya que utilizan conceptos y términos que son muy propios del ambiente

CAPITULO II

2. MARCO TEÓRICO DE REFERENCIA

2.1 GESTIÓN DE RED

Las redes de datos han evolucionado con el paso del tiempo ante la necesidad de satisfacer las demandas de los diferentes servicios de telecomunicaciones, que día a día necesitan un mayor ancho de banda y una mejor calidad de servicio para las nuevas aplicaciones que se han venido desarrollando hasta la actualidad. La tecnología de redes ha incrementado su complejidad generándose la necesidad de contar con una mejor administración de los recursos de estos sistemas, lo cual ha favorecido la evolución conjunta de la gestión de redes. La gestión de redes tiene como propósito la utilización y coordinación de los recursos para planificar, organizar, mantener, supervisar, evaluar, y controlar los elementos de las redes de datos para adaptarse a la calidad de servicio necesaria, a un determinado costo. Su campo de aplicación es amplio y de gran importancia dadas las características tecnológicas que poseen los sistemas de telecomunicaciones y los servicios que ofrecen, mantiene un cierto grado de complejidad al interactuar con sistemas heterogéneos que involucran diversos fabricantes con productos eminentemente propietarios, así como productos apegados a estándares en forma total o parcial.

2.1.1 ELEMENTOS DE UN SISTEMA DE GESTIÓN

La gestión de un entorno de telecomunicaciones es una aplicación de procesamiento de información, en la cual intervienen elementos fundamentales como son el gestor, el agente, el protocolo de gestión, y la base de información de gestión (MIB, Management Information Base), los cuales interactúan entre sí empleando el modelo gestor-agente.

- El gestor es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión en la cual se debe disponer de la MIB del dispositivo en gestión y una interfaz de usuario.
- El agente tiene la función de responder a las directivas enviadas por el gestor y lo realiza accesando a la MIB para manipular los objetos involucrados en la operación. El agente se encuentra ubicado en el dispositivo de telecomunicaciones gestionado.
- La MIB es el conjunto de objetos gestionados (el concepto de objeto es diferente al empleado en la programación orientada a objetos) que representan a los recursos de la red que permiten algún tipo de gestión en una forma abstracta. La MIB se encuentra ubicada en el dispositivo de telecomunicaciones, y una referencia de ésta es necesaria en el gestor.

- El protocolo es el conjunto de especificaciones y convenciones que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión. En la actualidad SNMP (Simple Network Management Protocol), forma parte del modelo de gestión de internet, y CMIP (Common Management Information Protocol), es parte del modelo de gestión OSI son los protocolos predominantes.

2.1.2 AREAS FUNCIONALES

El marco de gestión OSI [CCITT, X.701] define 5 áreas funcionales, en las cuales se divide la gestión de red:

- Gestión de fallas: Establece la generación de notificaciones específicas de error (alarmas), el registro de las notificaciones de error y la verificación de los recursos de red para trazar e identificar fallas.
- Gestión de configuración: Se distribuye en actividades de inicialización, instalación, y abastecimiento. Esto permite la colección de información de configuración y estado en demanda, proporcionando facilidades de inventario y además soporta el anuncio de cambios de configuración a través de notificaciones relevantes.
- Gestión de contabilidad: Consiste de actividades de recolección de

información de contabilidad y su procesamiento para propósitos de cobranza y facturación. Estas actividades establecen un límite contable para que un conjunto de costo se combinen con recursos múltiples y se utilicen en un contexto de servicio.

- Gestión de desempeño: Proporciona información en forma ordenada para determinar la carga del sistema y de la red bajo condiciones naturales y artificiales, proporcionando estadísticas y permitiendo actividades de planeación de configuración.
- Gestión de seguridad: Está relacionada con 2 aspectos de la seguridad del sistema: La gestión de seguridad misma, la cual requiere la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y reportar amenazas y rupturas en la seguridad. Y la seguridad de la gestión, la cual requiere la habilidad para autentificar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados a la información.

2.2 PROTOCOLOS DE ADMINISTRACION DE REDES

2.2.1 PROTOCOLO SNMP

El protocolo SNMP se utiliza principalmente para monitorizar y controlar el estado de los recursos conectados a las redes IP, en especial equipos de intercomunicación (conmutadores, enrutadores, modems, etc), aunque se puede usar en cualquier tipo de equipo que permita ejecutar un agente SNMP.

Ha sufrido numerosos cambios en los últimos años, pero las mas importantes son las siguientes:

SNMPv1 La primera versión del protocolo. Establecida en rfc 1157

SNMPv2C Autentificación basada en los llamados "community strings"

SNMPv3 La mas nueva e interesante, es el estándar de SNMP del futuro

El protocolo SNMP, es en principio una típica aplicación cliente-servidor, donde el servidor (el agente de SNMP) presenta información acerca de si mismo en un árbol jerárquico, información como el nombre del administrador, de la máquina, las configuraciones de sus tarjetas de red, etc.

El agente es un proceso llamado SNMPD, el cual permite la comunicación con la entidad gestora o también llamada NMS, para la comunicación se emplea el protocolo UDP, y generalmente escucha en los puertos 161 y 162.

El agente también esta capacitado para informar de acontecimientos inusuales en su entorno por medio de mensajes "Traps", los eventos que origina un trap pueden ser un reinicio, que haya demasiado tráfico en la red, un router que deja de responder. Los traps los envía el agente sin haberlos

solicitado previamente la entidad gestora.

OPERACIONES BASICAS DE SNMP

Para solicitar información del agente, el manager emplea un mecanismo denominado get-request (petición-consulta), a lo que el agente responde con un get-response (petición-respuesta).

En la figura 1, se muestran las principales operaciones del protocolo SNMP

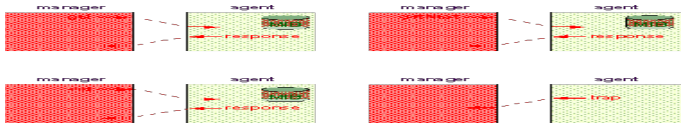
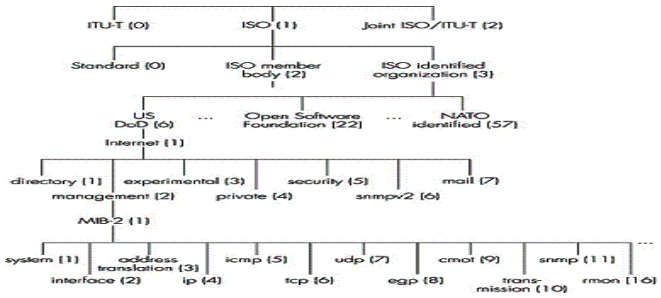


Fig. 1 Operaciones del protocolo SNMP.

Toda la información del agente se guarda en una base de datos denominada Management Information Base (MIB), formando una estructura de árbol, y presentada en forma de objetos, siendo la raíz el nodo .

En la Fig. 2 se muestra un parte del árbol de variables.



CONTROL DE LA SEGURIDAD

Se debe tener un control sobre quien puede y quien no puede ver/realizar cambios en esta base de datos llena de información útil. Básicamente el método de autentificación se basa en community strings. Los community strings son una especie de claves (sin nombre de usuario) que se asigna a una determinado operación, que puede ser una de dos: leer o escribir a la MIB

El control de acceso ha ido evolucionando con las diferentes versiones de SNMP.

En la versión SNMPv1, una vez conocido el valor del community string, se tiene acceso total a la base de datos, pudiendo leer de la misma ó modificarla, según sea el caso. Es interesante hacer notar que el manager envía la clave al agente sin encriptar, en codigo ASCII, con el riesgo que eso conlleva. Los community strings por defecto son "public" y "private".

En la versión SNMPv2 se discutieron varios modelos de autentificación, empezando con uno basado en listas de control de acceso, en el cual los derechos que tiene cada manager sobre el agente se basan en su dirección IP, en diversas claves de autentificación, en la acción solicitada por el manager (get o set), etc. Actualmente se ha pasado a otro modelo denominado USEC, User based Security Model, mejorando

considerablemente la autentificación, control de acceso y privacidad de todo el sistema.

APLICACIÓN

Como se ha mencionado el SNMP se basa en un servidor (agente), el SNMPD. Para el cliente existen varias herramientas que le permiten consultar la MIB. Normalmente un administrador de red tendrá una representación gráfica, de los valores consultados de la MIB.

Una utilidad básica para trabajar con una MIB, es el Visualizador de MIB (MIB Browser, por ejemplo el de la compañía MG-soft).

Por último, mediante el SNMP se puedes obtener información muy valiosa sobre un host, como son las interfaces de red, las tablas de encaminamiento, datos del sistema operativo, etc. Analizando estos datos se pueden deducir las tasas de paquetes enviados y recibidos.

El SNMP permite también reiniciar la máquina, cambiar las variables e incluso en algunas situaciones se puede ejecutar programas en el host.

2.2.2 PROTOCOLO CMIP

El Protocolo de administración de información común (CMIP) es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes. CMIP se basa en el

MODELO OSI (*Open Systems Interconnection*) y es definido por la serie de recomendaciones ITU-T X.700.

CMIP define la información de la gerencia en términos de objetos administrados y permite tanto la modificación como las acciones sobre objetos manejados. Se describen usando GDMO y los objetos son identificados por un nombre distinguido (DN), similar en concepto al directorio X.500.

Los NMS pueden realizar las operaciones siguientes:

- CREAR - crear una instancia de un objeto manejado.
- CANCELACIÓN - suprimir una instancia de un objeto manejado.
- CONSEGUIR - solicitar el valor de una instancia manejado del objeto.
- CANCEL_GET - cancelar un excepcional CONSIGUEN la petición.
- SISTEMA - fijar el valor de una instancia de de un objeto manejado.
- ACCIÓN - solicitar una acción para ocurrir según lo definido por el objeto manejado.

El agente administrador puede realizar esta operación:

- EVENT_REPORT - enviar notificaciones o alarmar a los NMS.

CMIP también proporciona buena seguridad (autorización de la ayuda, control de acceso y registros de la seguridad) y un reporte flexible de las condiciones inusuales de la red.

2.3 REDES VIRTUALES PRIVADAS

Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet son lo mejor que se ha implementado.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de

intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES)

2.3.1 TIPOS DE VPN

VPN DE ACCESO REMOTO

Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura «dial-up» (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos modems.

VPN PUNTO A PUNTO

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y

establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamada tecnología de túnel o tunneling.

TUNNELING

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin

cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida. Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos.

Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling. Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure Shell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

VPN INTERNA WLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

BENEFICIOS DE VPN

Las VPN son una salida al costo que puede significar el pagar una conexión de alto coste, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Los datos son codificados o cifrados y recién enviados a través de la conexión, para de esa manera asegurar la información y el password que se esté enviando.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Mas aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red

La tecnología de túneles esta basado en estándares. Esta tecnología permite transmitir datos entre dos redes similares. A esto también se llama "encapsulación", es decir, a la tecnología que coloca algún tipo de paquetes dentro de otro protocolo (TCP). Aparte de todo esto, también se añade otra información necesaria para poder descifrar la información que se encuentra codificada. Estos paquetes llegan a su destino después de haber atravesado Internet, pero para verificar que ha llegado al destino correcto se realiza un proceso de autentificación.

Las VPNs son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre si.

Pero observándolo desde el punto de vista de los usuarios particulares de

Internet, como son los estudiantes o investigadores que utilizan el Internet como un medio de comunicación, de compartimiento de información, este tipo de redes perjudican este desarrollo, debido a varios factores como son, el consumo de ancho de banda y el consumo de direcciones IP.

TIPOS DE CONEXION

CONEXIÓN DE ACCESO REMOTO

Una conexión de acceso remoto es realizada por un cliente o un usuario de un computador que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y este se autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente.

CONEXIÓN VPN ROUTER A ROUTER

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y tambien sirve para la intranet

CONEXIÓN VPN FIREWALL ASA A FIREWALL ASA

Una conexión VPN Firewall ASA a Firewall ASA es realizada por un Firewall ASA, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier usuario en Internet. El Firewall ASA que realiza la llamada se autentica ante el Firewall ASA que responde y este a su vez se autentica ante el Firewall ASA que realiza la llamada.

2.3.2 PROTOCOLOS UTILIZADOS EN LAS VPN

POINT-TO-POINT TUNNELING PROTOCOL

Fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los

usuarios se conectan a su proveedor y luego “llaman” al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS.

Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego “llama” al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá

acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header IP, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, Frame Relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor.

Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. Las capas del encapsulamiento PPTP son: Paquete de envío, Header IP, HeaderGREv2, datagramas de carga.

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, estándar en el que se intercambia un “secreto” y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un estándar propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP

(Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

IPSEC

IPSEC trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSEC da soporte a ambos de una manera uniforme.

IPSEC provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del Header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al Header.

AH sigue al Header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del Header IP.

El Header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del Header IP, no garantiza nada sobre el mismo, sólo la carga.

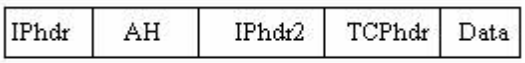
Una división de la funcionalidad de IPSEC es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los Headers de seguridad son antepuestos a los de la capa de transporte, antes de que el Header IP sea incorporado al paquete. En otras palabras, AH cubre el Header TCP y algunos campos IP, mientras que ESP cubre la encriptación del Header TCP y los datos, pero no incluye ningún campo del Header IP.
- El modo de túnel es usado cuando el Header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el

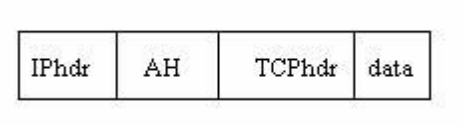
paquete entero, incluyendo el Header IP entre los extremos, agregando al paquete un Header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSEC son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel es:



Un ejemplo de paquete AH en modo transporte es:



Como ESP no puede autentificar el Header IP más exterior, es muy útil combinar un Header AH y ESP para obtener lo siguiente:

Este tipo de paquete se denomina Transport Adjacency.

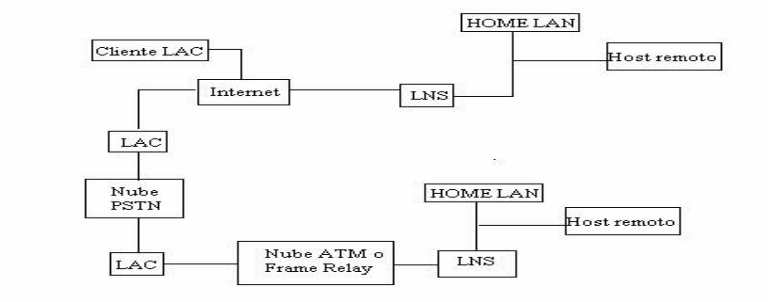
La versión de entunelamiento sería:

L2TP

Lyer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos

corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:



Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

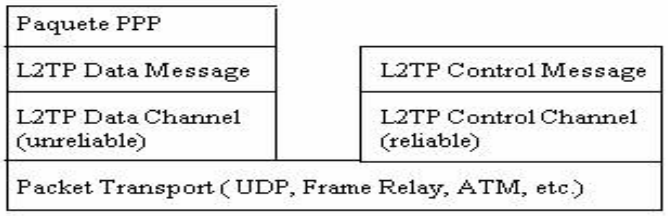
Un cliente LAC, una máquina que corre nativamente L2TP, puede participar

también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L-2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.



Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que

son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la

respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

2.4 SISTEMAS OPERATIVOS LINUX

Linux es, a simple vista, un Sistema Operativo. Es una implementación de libre distribución UNIX para computadoras personales (PC), servidores, y estaciones de trabajo. Fue desarrollado para el i386 y ahora soporta los procesadores i486, Pentium, Pentium Pro y Pentium II, así como los clones AMD y Cyrix. También soporta máquinas basadas en SPARC, DEC Alpha, PowerPC/PowerMac, y Mac/Amiga Motorola 680x0.

Como sistema operativo, Linux es muy eficiente y tiene un excelente diseño. Es multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido; protege la memoria para que un programa no pueda hacer caer al resto del sistema; carga sólo las partes de un programa que se usan; comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria; usa un sistema de memoria virtual por páginas; utiliza toda la memoria libre para cache; permite usar bibliotecas enlazadas tanto estática como dinámicamente; se distribuye con código fuente; usa hasta 64 consolas virtuales; tiene un sistema de archivos avanzado pero puede usar los de los otros sistemas; y soporta redes tanto en TCP/IP como en otros protocolos.

2.4.1 HISTORIA DE LINUX

LINUX hace su aparición a principios de la década de los noventa, era el año 1991 y por aquel entonces un estudiante de informática de la Universidad de Helsinki, llamado Linus Torvalds empezó, -como una afición y sin poderse imaginar a lo que llegaría este proyecto, a programar las primeras líneas de código de este sistema operativo llamado LINUX.

Este comienzo estuvo inspirado en MINIX, un pequeño sistema Unix desarrollado por Andy Tanenbaum. Las primeras discusiones sobre Linux fueron en el grupo de noticias Comp os Minix, en estas discusiones se hablaba sobre todo del desarrollo de un pequeño sistema Unix para usuarios de Minix que querían mas.

Linus nunca anuncio la versión 0.01 de Linux (agosto 1991), esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que uno tenia acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus anuncio la primera versión "Oficial" de Linux, -versión 0.02. Con esta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C) pero no mucho mas funcional. En este estado de desarrollo ni se pensaba en los términos soporte, documentación, distribución .Después de la versión 0.03, Linus salto en la

numeración hasta la 0.10, más y mas programadores a lo largo y ancho de internet empezaron a trabajar en el proyecto y después de sucesivas revisiones, Linus incremento el numero de versión hasta la 0.95 (Marzo 1992). Mas de un año después (diciembre 1993) el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 no llego hasta el 14 de marzo de 1994. Desde entonces no se ha parado de desarrollar, la versión actual del núcleo es la 2.2 y sigue avanzando día a día con la meta de perfeccionar y mejorar el sistema.

Linus Benedict Torvalds

Linus Benedict Torvalds nació en Helsinki, Finlandia, el año 1969. Empezó a "trabajar" con computadoras a los 10 años, cuando su abuelo le compró un Comodore el año 1980. Éste buen señor era un matemático y estadista. Trabajaba a la Universidad y fue quién "enganchó" al mundo de los computadores a nuestro buen amigo Linus.

Con el paso del tiempo, Linus pasó a tener un Sinclair QL, un gran ordenador de Clive Sinclair (creador del conocido Spectrum), que tenía algún pequeño error de diseño. Linus se sintió especialmente atraído por esta máquina, después de crear aplicaciones para ésta computadora y de haber retocado su hardware con la finalidad de adaptarlo a sus necesidades. El problema que tenía dicha máquina era que los recursos eran insuficientes para poder llevar a la práctica los planes de Linus. Además, no era un

equipo compatible. Así pues, el mes de enero de 1991 compró su primer PC, un 386.

En 1988 fue cuando Linus entró a la Universidad. Este mismo año fue cuando un sistema operativo didáctico, basado en Unix y creado por Andy Tannenbaum, empezó a cobrar importancia. Dicho sistema operativo era el famoso Minix.

Linus Tannenbaum cometió un error en su sistema operativo. Era demasiado limitado, tanto técnicamente como políticamente, es decir, en ningún momento tuvo en cuenta la posibilidad de incluir Minix al proyecto GNU (creado el año 1983 por Richard Stallman). En realidad, la creación de Andy Tannenbaum estaba pensada para ser distribuida comercialmente. Su principal error fue ceder todos los derechos a Prentice Hall, que empezó a cobrar 150 dólares por licencia.

Así pues, Linus tomó la decisión de cambiar esta política debido a que el sistema Minix era ideal para los estudiantes de sistemas operativos, y su precio era considerablemente alto. Llegamos de nuevo al año 1991, cuando Linus se acabó de comprar su primer 386. En aquellos momentos, la intención de nuestro amigo era clara: crear un nuevo Kernel de UNIX basado en el Kernel de Minix y modificarlo periódicamente de manera que fuera capaz de ejecutar aplicaciones GNU.

2.4.2 CARACTERISTICAS DE LINUX

- Multitarea: La palabra multitarea describe la habilidad de ejecutar varios programas al mismo tiempo.
- LINUX utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados, siendo el sistema operativo el encargado de ceder tiempo de microprocesador a cada programa.
- Multiusuario: Muchos usuarios usando la misma maquina al mismo tiempo.
- Multiplataforma: Las plataformas en las que en un principio se puede utilizar Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II, Amiga y Atari, también existen versiones para su utilización en otras plataformas, como Alpha, ARM,MIPS, PowerPC y SPARC.
- Multiprocesador: Soporte para sistemas con mas de un procesador esta disponible para Intel y SPARC.
- Funciona en modo protegido 386.
- Protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.

- Carga de ejecutables por demanda: Linux sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.
- Política de copia en escritura para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: A una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio. Este limite se puede aumentar fácilmente con el cambio de unas cuantas líneas en el código fuente.
- La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta

puede a su vez ser reducida cuando se ejecuten grandes programas.

- Librerías compartidas de carga dinámica (DLL's) y librerías estáticas.
- Se realizan volcados de estado (core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.
- Compatible con POSIX, System V y BSD a nivel fuente.
- Emulación de iBCS2, casi completamente compatible con SCO, SVR3 y SVR4 a nivel binario.
- Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente. Hay algunos programas comerciales que están siendo ofrecidos para Linux actualmente sin código fuente, pero todo lo que ha sido gratuito sigue siendo gratuito.
- Control de tareas POSIX.
- Pseudo-terminales (pty's).
- Emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática.

Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático. Por supuesto, si el ordenador ya tiene una FPU (unidad de coma flotante), esta será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

- Soporte para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.
- Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.
- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no es necesario ningún comando especial para usar la partición MS-

DOS, esta parece un sistema de archivos normal de Unix (excepto por algunas restricciones en los nombres de archivo, permisos, y esas cosas). Las particiones comprimidas de MS-DOS 6 no son accesibles en este momento, y no se espera que lo sean en el futuro. El soporte para VFAT (WNT, Windows 95) ha sido añadido al núcleo de desarrollo y estará en la próxima versión estable.

- Un sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.
- Soporte en sólo lectura de HPFS-2 del OS/2 2.1
- Sistema de archivos de CD-ROM que lee todos los formatos estándar de CD-ROM.
- TCP/IP, incluyendo ftp, telnet, NFS, etc.
- Appletalk.
- Software cliente y servidor Netware.
- Lan Manager / Windows Native (SMB), software cliente y servidor.
- Diversos protocolos de red incluidos en el kernel: TCP, IPv4, IPv6, AX.25, X.25, IPX, DDP, Netrom, etc.

¿QUÉ SON LAS "DISTRIBUCIONES" DE GNU/LINUX?

Una distribución es un modo de facilitar la instalación, la configuración y el mantenimiento de un sistema GNU/Linux. Al principio, las distribuciones se limitaban a recopilar software libre, empaquetarlo en disquetes o CD-ROM y redistribuirlo o venderlo.

Ahora las grandes distribuciones -RedHat, SuSE, Caldera, Mandrake, Corel Linux, Ubuntu, TurboLinux...- son potentes empresas que compiten entre sí por incluir el último software, a veces también software propietario, con instalaciones gráficas capaces de auto detectar el hardware y que instalan un sistema entero en unos cuantos minutos sin apenas preguntas.

Entre las distribuciones de GNU/Linux, destaca el proyecto Debian/GNU. Debian nace como una iniciativa no comercial de la FSF, aunque luego se independiza de ésta y va más allá del propio sistema GNU/Linux. Es la única de las grandes distribuciones que no tiene intereses comerciales ni empresariales. Son sus propios usuarios, muy activos, quienes mantienen la distribución de modo comunitario, incluidas todas sus estructuras de decisión y funcionamiento. Su objetivo es recopilar, difundir y promover el uso del software libre. Reúne el mayor catálogo de software libre, todos ellos probados, mantenidos y documentados por algún desarrollador voluntario.

En una distribución hay todo el software necesario para instalar en un

ordenador personal; servidor, correo, ofimática, fax, navegación de red, seguridad, etc.

LINUX FRENTE A LOS OTROS SISTEMAS OPERATIVOS

Linux es una muy buena alternativa frente a los demás sistemas operativos. Más allá de las ventajas evidentes de costo, ofrece algunas características muy notables.

En comparación con las otras versiones de Unix para PC, la velocidad y confiabilidad de Linux son muy superiores. También está en ventaja sobre la disponibilidad de aplicaciones, ya que no hay mucha difusión de estos otros Unixes (como Solaris, XENIX o SCO) entre los usuarios de PC por sus altos costos.

Comparado con sistemas operativos como los diferentes Microsoft Windows, Linux también sale ganando. Los bajos requisitos de hardware permiten hacer un sistema potente y útil de aquel 486 que algunos guardan en un armario. Esta misma característica permite aprovechar al máximo las capacidades de las computadoras más modernas. Es poco práctico tener una PC con 16 Mb de RAM y ponerle un sistema operativo que ocupa 13 (que es lo que reporta sobre Windows 95 el System Information de Symantec). No solo es superior respecto a el sistema de multitarea y de administración de memoria, sino también en la capacidades de networking

(conectividad a redes) y de multiusuario (aún comparando con sistemas multiusuario como NT). La única desventaja de Linux frente a estos sistemas, es la menor disponibilidad de software, pero este problema disminuye con cada nuevo programa que se escribe para el proyecto GNU, y con algunas empresas que están desarrollando software comercial para Linux (por ej., Corel).

2.5 ESCRITORIO REMOTO

El acceso remoto a una computadora era una función que podían realizar primeras grandes computadoras que poseían un número de terminales de texto unidos a éstas a través de interfaces simples, básicamente cables.

El desarrollo de las redes de telecomunicaciones permitió que poco a poco fueron desapareciendo estos terminales de texto, siendo sustituidos por otras computadoras (generalmente más pequeñas) capaces de emular la misma funcionalidad a través de una aplicación, denominada emulador de terminal, siendo, por lo tanto, las primeras tecnologías de acceso remoto a computadoras, como Telnet y SSH, popularizadas inicialmente en entornos Unix.

Cerca de la década de los noventa, las interfaces de usuario sufren una revolución, abandonando la interacción textual en favor de una interacción

más gráfica. Debido a esta revolución surgen dos tecnologías nuevas:

Los terminales gráficos, también denominados clientes ligeros o thin-client. Evolución de los viejos terminales de texto unidos por cables.

Los escritorios gráficos. Dos escritorios gráficos muy populares son los creados para Apple Macintosh y MS-DOS (Microsoft Windows). Nótese que estos escritorios gráficos solamente podían ser utilizados directamente en la computadora, por tanto, aún no son escritorios remotos.

El primer entorno operativo de escritorio remoto es X-Window, originalmente desarrollado por el Massachusetts Institute of Technology (MIT) con el nombre de proyecto Athena en 1984. El objetivo inicial era lograr la compatibilidad en materia de escritorios remotos de los diversos fabricantes. Este objetivo resultó ampliamente logrado con su aceptación por parte de dichos fabricantes.

En 1988, se creó la fundación X-Consortium (hoy conocida como X.Org) como organismo encargado del desarrollo y estandarización de X-Window. El éxito de este sistema aún perdura siendo el núcleo de todos los escritorios (tanto locales como remotos) de los sistemas Unix y Linux. También ha tenido alcance en otros sistemas operativos existiendo clientes para Windows y MacOS.

2.5.1 RDP

Remote Desktop Protocol (RDP) es un protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información ingresada por el usuario en el terminal mediante el ratón ó el teclado).

El modo de funcionamiento del protocolo es sencillo. La información gráfica que genera el servidor es convertida a un formato propio RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal. En cuanto a la introducción de órdenes en el terminal por parte del usuario, las teclas que pulse el usuario en el teclado del terminal así como los movimientos y pulsaciones de ratón son redirigidos al servidor, permitiendo el protocolo un cifrado de los mismos por motivos de seguridad.

El protocolo también permite que toda la información que intercambien cliente y servidor sea comprimida para un mejor rendimiento en las redes menos veloces. Pues es la única de las soluciones de clientes ligeros analizadas que nos permite utilizar este protocolo para que los terminales puedan actuar como clientes de servidores Windows, lo que puede ser interesante en multitud de ambientes de trabajo en los que se utilizan

servidores Microsoft.

Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de Windows, no se verá lo que el usuario está realizando de forma remota.

2.5.2 VNC

VNC es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto: Es posible compartir la pantalla de una máquina de "cualquier" sistema operativo conectando desde cualquier otro ordenador o dispositivo que disponga de un cliente VNC portado.

La versión original del VNC se desarrolló en Reino Unido, concretamente en los laboratorios AT&T, en Cambridge. El programa era de código abierto por lo que cualquiera podía modificarlo y existen hoy en día varios programas para el mismo uso.

En la enseñanza VNC sirve para que el profesor comparta su pantalla con los alumnos, por ejemplo en un laboratorio. También puede usarse para que

un técnico ayude a un usuario inexperto, el técnico ve remotamente el problema que reporta el usuario.

El programa servidor suele tener la opción de funcionar como servidor HTTP para mostrar la pantalla compartida en un navegador con soporte de Java. En este caso el usuario remoto (cliente) no tiene que instalar un programa cliente de VNC, éste es descargado por el navegador automáticamente.

2.5.3 X11

El sistema de ventanas X fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el que está en uso actualmente.

X es el encargado de mostrar la información gráfica y es totalmente independiente del sistema operativo. El sistema de ventanas X distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se

ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Debido a este esquema cliente-servidor, se puede decir que X se comporta como una terminal gráfica virtual.

El hecho que exista un estandar definido para X permite que se desarrollen servidores X (XServers) para distintos Sistemas Operativos, plataformas, Hardwares, etc. lo que hace que el código sea muy portable. Por ejemplo. permite tener Xclients ejecutándose en potente servidor UNIX mientras los resultados son visualizados en una PC de escritorio con cualquier otro sistema operativo funcionando.

La comunicación entre el Xclient y el Xserver se realiza por medio de un protocolo conocido como Xprotocol, que constituye una serie bytes interpretados como comandos básicos para generar ventanas, posicionarlas, o controlar eventos. Los Xclients acceden al Xprotocol mediante el uso de una librería llamada Xlib, que evita al programador de Xclients tener que lidiar con el código binario del Xprotocol. Sinembargo los aspectos de decoración de ventana y manejos de ventanas no estan definidos en esta librería. X NO ES UN WINDOWS MANAGER, necesita de uno para controlar el manejo de ventanas. Esto trae la ventaja de que permite al usuario instalar el administrador de ventanas que más le agrade, e incluso tener

varios instalados eligiendo el más apropiado a la hora de acceder a X. También trae la ventaja de que hace de X estrictamente un sistema gráfico, de tal modo que un Xclient podría estar enviando un gráfico a una pantalla, a una impresora o a cualquier otro hardware sin darse cuenta, flexibilizando la salida gráfica. Por otro lado, la desventaja que trae el hecho de no tener un único Windows manager es que los programadores de Xclients que desean hacer uso de los recursos de los Windows Manager (botones, barras de deslizamientos, etc.) deben elegir un Windows manager específico para programar y contar que el usuario tenga por los menos las librerías de dicho Windows manager instalado.

CAPITULO III

3. PROYECTO TEMÁTICO

3.1 PLANTEAMIENTO DEL PROYECTO TEMÁTICO

El desarrollo de este proyecto ha conllevado a la realización de diferentes etapas para la elaboración de una propuesta de una herramienta que sea capaz de administrar remotamente los servidores en una red local.

Dentro de las etapas que se realizaron para dicho proyecto podemos mencionar:

Etapa 1: Investigación tecnológica:

En esta etapa se procedió a realizar una consulta a varios docentes y empresas de amistades que se visitaron para consultar el tipo de herramientas utilizadas para la gestión de los equipos en red, dentro de las empresas visitadas están Digicel El Salvador.

Como resultado de esta etapa se obtuvo un listado generalizado de varias herramientas que se encuentran en este ambiente de administración de redes. Así como de protocolos para administrar equipos remotamente.

Etapa 2: Implementación de pruebas

Durante el desarrollo de esta fase, se definió como meta, la instalación de varias herramientas para evaluarse, entre ellas podemos mencionar: Cacti, Orion SolarWinds, Nagios, Loriot pro, SNMP Trap Watcher de BTT Softwarey SNMP, Watcher de DartwareOtra, NET-SNMP.

De estas herramientas, se evaluaron los aspectos siguientes:

- Integración con la mayoría de plataformas de software operativos
- Facilidad de uso
- Gestión remota de los sistemas control y monitoreo de los componentes principales de los equipos, como Memoria, Procesador, Disco Duro, entre otros.

- Monitoreo de aplicaciones
- Gestión de alertas

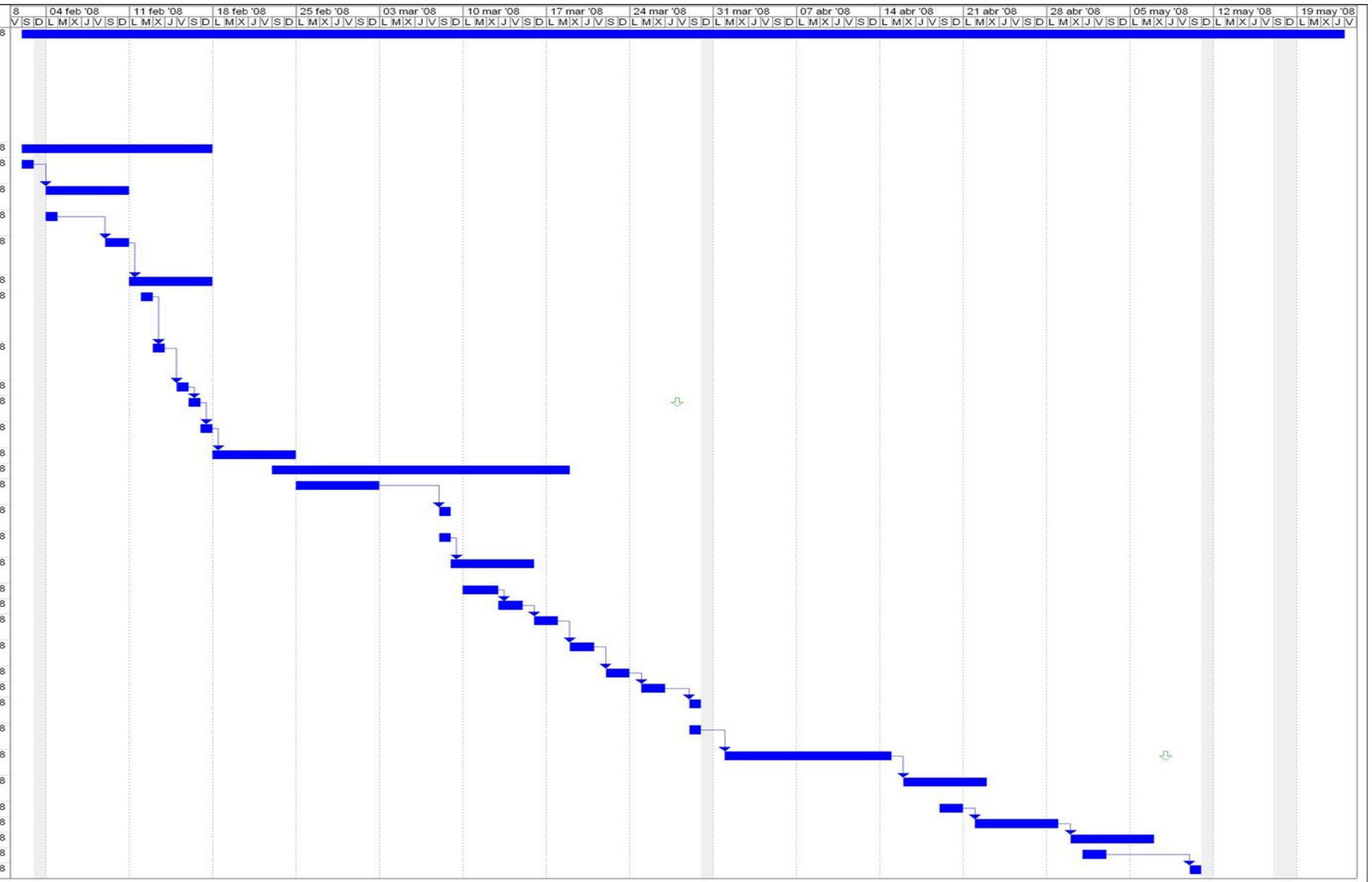
Algunos productos basados en su documentación técnica fueron descartados de estas pruebas ya que no cumplían.

Etapa 3: Evaluación Técnica

Como resultado de la etapa anterior, obtuvimos un listado mas pequeño de productos que serán los mas fuertes candidatos para que sean considerados como la herramienta a proponer. En esta etapa se monta un laboratorio para realizar las pruebas con el equipo de hardware adecuado para poder realizar las instalaciones y configuraciones de los diferentes productos asi como interactuar con las diferentes interfaces de cada uno de ellos.

3.2 CRONOGRAMA DEL PROYECTO

Id	Nombre de tarea	Duración	Comienzo
1	Implementacion de una herramienta para la gestacion remota de servidores a traves de una red privada virtual basada en linux con fines academicos para los estudiantes de la carrera Tec. En Ing. En Redes Computacionales.	106 dias	sáb 02/02/08
2	primera etapa	15 dias	sáb 02/02/08
3	asistir a la 1ª reunion de seguimiento (UTEC)	1 dia	sáb 02/02/08
4	planteamiento de formulacion de proyectos	7 dias	lun 04/02/08
5	realizar un resumen y evaluacion de datos abtenidos.	1 dia	lun 04/02/08
6	realizacion de pruebas y evaluacion de software para la gestion remota de servidores	2 dias	sáb 09/02/08
7	formulacion del tema	7 dias	lun 11/02/08
8	Realizacion de pruebas de sist. Operativo linux ubuntu 7.10 y windows 2003 a traves de software	1 dia	mar 12/02/08
9	pruebas de enlace de VPN a traves de software de VPN, VNS	1 dia	mié 13/02/08
10	evaluacion de protoclolos	1 dia	vie 15/02/08
11	asistir a la 2ª reunion de seguimiento (UTEC)	1 dia	sáb 16/02/08
12	intalacion y pruebas de servidor	1 dia	dom 17/02/08
13	inicio de documentacion marco teoric	7 dias	lun 18/02/08
14	segunda etapa	25 dias	sáb 23/02/08
15	inicio de documentacion marco teorico de referencia.	7 dias	lun 25/02/08
16	asistir a la 3ª reunion y seguimiento(UTEC)	1 dia	sáb 08/03/08
17	entrega de la primera documentacion	1 dia	sáb 08/03/08
18	inicio de documentacion planteamiento del proyecto tematico	7 dias	dom 09/03/08
19	cronogramna del proyecto	3 dias	lun 10/03/08
20	documentacion tecnica	2 dias	jue 13/03/08
21	evaluacion tecnica y economica	2 dias	dom 16/03/08
22	tecnologia y recursos seleccionados	2 dias	mié 19/03/08
23	presupuesto proyectado	2 dias	sáb 22/03/08
24	oferta tecnica y economica	2 dias	mar 25/03/08
25	entrega de 2ª parte del proyecto	1 dia	sáb 29/03/08
26	asistir a 4ª reunion de seguimiento	1 dia	sáb 29/03/08
27	evaluacion y entrega de correccion de Cap. III Proyecto tematico.	14 dias	mar 01/04/08
28	inicio de documentacion diseño y elaboracion del proyecto	7 dias	mié 16/04/08
29	articulo del prototipo (texto)	2 dias	sáb 19/04/08
30	presentacion del prototipo	7 dias	mar 22/04/08
31	evidencias del proyecto	7 dias	mié 30/04/08
32	generalidades del proyecto	2 dias	jue 01/05/08
33	entrega del documento final	1 dia	sáb 10/05/08



Proyecto: Proyect1_ricardo
Fecha: dom 01/06/08

Tarea · Progreso · Hito · Resumen · Tarea resumida · Hito resumido · Progreso resumido · División · Tareas externas · Resumen del proyecto · Agrupar por síntesis · Fecha límite

Página 1

3.3 DOCUMENTACIÓN TÉCNICA

En esta sección se detallan todos los requerimientos técnicos necesarios para la implementación de las herramientas propuestas para este proyecto, todos estos detalles son proporcionados por los fabricantes de cada producto, de los cuales podemos mencionar:

Win 2003 Server R2 o Linux Ubuntu Server

Servidor Web, IIS o Apache

Active Page Server o PHP

ASP.net

SNMPtrap

De igual forma es necesario contar con una base de datos para almacenar las estadísticas de gestión, como Microsoft SQL o MySQL

mas detalles acerca de el productos ver el Anexo 2.

3.4 EVALUACIÓN TÉCNICA Y ECONÓMICA

EVALUACION TECNICA DEL PRODUCTO SERA CONSIDERADO COMO APROBADO SI ALCANZA UNA PONDERACION MINIMA DEL 85%

CARACTERISTICAS	PARAMETRO O VALORACION REQUERIDA	PESO	OPCIONES A EVALUAR					
			CACTI		NAGIOS		SOLARWINDS	
			CALIFICACION	PUNTAJE	CALIFICACION	PUNTAJE	CALIFICACION	PUNTAJE
Monitoreo de la banda ancha	Indispensable	10%	2	20	2	20	2	20
Monitoreo de Discos Duros	Indispensable	12%	1	12	2	24	2	24
monitoreo de Utilización de Cpu	indispensable	12%	1	12	2	24	1	12
Monitoreo de uso de Memoria	Indispensable	12%	2	24	1	12	2	24
Interfaz web grafica	Indispensable	10%	2	20	1	10	2	20
Compatibilidad con diferentes SO y tecnologias de hardware	Indispensable	10%	2	20	2	20	1	10
Servicio de notificaciones y reportes automatizado	No indispensable	7%	1	7	1	7	1	7
Alto nivel de seguridad	No indispensable	5%	2	10	2	10	2	10
Escalabilidad	No indispensable	5%	1	5	1	5	2	10
Facil configuracion de alertas de red	Indispensable	5%	1	5	2	10	2	10
Vigilancia de nodos de red	Indispensable	12%	2	24	2	24	2	24
TOTALES		100%		159		166		171
PONDERACION FINAL				79.5		83		85.5
RESULTADO OBTENIDO			REPROBADO		REPROBADO		APROBADO	
CALIFICACION	(0), si no cumple o no especifica que cumple.				(1), cumple a medias sin perder la funcionalidad			
	(2), cumple o supera lo requerido							

3.5 TECNOLOGÍA Y RECURSOS SELECCIONADOS

El resumen de los productos técnicos a utilizar en base a la evaluación anterior son los siguientes:

Producto seleccionado: SolarWinds Orion SL100 (SQL incluido)

Fabricante: Solarwinds

Sistema Operativo: Windows server 2003

RECURSOS DE HARDWARE NECESARIOS

Procesador: 2.0 Ghz

Memoria: 1 Gb

Disco duro: 2 Gb

Estos son los recursos recomendados por el fabricante, para poder controlar una cantidad de equipos de 500, para una mayor cantidad, es necesario considerar un perfil de hardware superior.

3.6 PRESUPUESTO PROYECTADO

Cliente:	Universidad Tecnológica de El Salvador	
Dirección:	Calle Arce San Salvador	

Cantidad	Descripción	Precio unitario	Total
1	SolarWinds Orion Performance Monitor SL100	$2475.00	$2475.00
		Total	$2475.00

3.7 OFERTA TÉCNICA Y ECONÓMICA

3.7.1 OFERTA TÉCNICA

TECNOTECH

San Salvador

Universidad Tecnológica de El Salvador

Calle Arce # 1120 San Salvador, El Salvador

A quien Interese:

Sirva la presente para saludarles y a la vez desearles el mejor de los éxitos en el desempeño de sus labores profesionales, es grato para nosotros saludarles a través de la presente deseando que todas sus actividades sean de éxito.

Como grupo estamos dedicados al diseño de material académico empleando la aplicación de Solarwinds, nuestra misión esta enfocada en la creación de una herramienta de apoyo para las prácticas de laboratorio del área de la carrera Técnico en Ingeniería de Redes es importante mencionar que contamos con el personal técnico con los conocimientos en el área.

Esperando servirle muy pronto

DESCRIPCIÓN DE LA PROPUESTA

Debido a que la tecnología se encuentra en constante crecimiento y cada día es más indispensable el uso de las computadoras, es necesario mantener una estricta seguridad y un buen control de las aplicaciones que a diario se utilizan en nuestra empresa.

Es por eso que hemos decidido trabajar con una herramienta que le facilite al administrador de nuestra red mantener un control estricto y de manera remota y centralizada todo trafico que circula dentro de nuestra red empresarial.

Seguidamente se procederá a la implementación de la aplicación Solarwinds que posee una interfaz web que le facilita su uso, además que es capaz de mantener un monitoreo de trafico y gestión de red con diferentes plataformas de software como lo es Windows y Linux.

PROYECCIONES

- Se podrá monitorear todo tráfico que circula dentro de la red.
- Se podrá incrementar la seguridad de los datos.
- Se podrá gestionar nuestra red empresarial de manera remota.

CARACTERÍSTICAS DE SOLARWINDS ORION

Orion proporciona un robusto conjunto de características que le permite aumentar el rendimiento de la red y disponibilidad, al tiempo que mejora la eficiencia de esta. Además, es increíblemente fácil de utilizar y es altamente escalable y ampliable.

Con Orion puede visualizar miles de nodos e interfaces desde una sola página web.

Además permite gestionar y mantener a la disponibilidad de la red herramientas para garantizar que su red está siempre funcionando al máximo rendimiento.

GARANTÍA

Se contara con un ambiente en el cual existan los servicios descritos anteriormente.

INVALIDACIÓN DE LA GARANTÍA

No se concederá garantía por mala administración de los recursos.

3.7.2 OFERTA ECONÓMICA

TECNOTECH

San Salvador

Universidad Tecnológica de El Salvador

Calle Arce # 1120 San Salvador, El Salvador C. A.

A quien interese:

Sirva la presente para saludarles y a la vez desearles el mejor de los éxitos en el desempeño de sus labores profesionales, es grato para nosotros saludarles a través de la presente deseando que todas sus actividades sean de éxito.

Como grupo estamos dedicados al diseño de material académico empleando la aplicación de Solarwinds, nuestra misión esta enfocada en la creación de una herramienta de apoyo para las prácticas de laboratorio del área de la carrera Técnico en Ingeniería de Redes es importante mencionar que contamos con el personal técnico con los conocimientos en el área.

Esperando servirle muy pronto

COMPONENTES DE LA OFERTA ECONÓMICA

Cliente: Universidad Tecnológica de El Salvador Dirección: Calle Arce San Salvador	

Cantidad	Descripción	Precio unitario	Total
1	Computadora Dell Power Edge T1O5	$1128.00	$1128.00
1	Windows 2003 server	$499.00	$499.00
1	SolarWinds Orion Performance Monitor SL100	$2475.00	$2475.00
1	Configuracion	$1000.00	$1000.00
		Total	$5102.00

Tiempo estimado de implementación: 4 días

CAPITULO IV

4. PROPUESTA

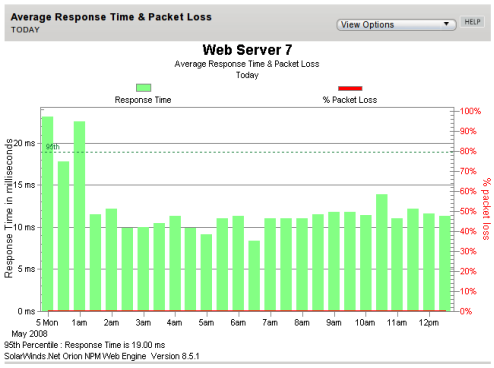
4.1 ARTICULO DEL PROTOTIPO

La Administración remota de Redes

Dentro de los planes de estudio de las carreras técnicas de la Universidad Tecnológica, se cubren aspectos de instalación, configuración y administración de servidores y otros aspectos técnicos, sin embargo, los aspectos de administración de redes como tal, no es enfocado desde el uso de una herramienta específica; y no se cuenta con una implementación de un producto de este tipo que le permita a los estudiantes realizar prácticas bajo un esquema administrativo global de una red. Es por ello que se propone este proyecto como respuesta a la necesidad de realización de practicas relacionadas con gestión remota de servidores, esta herramienta será de gran utilidad para los alumnos de la materia administración de redes, ya que podrán interactuar con servidores de monitoreo y gestión.
Este material estará disponible en los laboratorios de la Universidad Tecnológica de El Salvador y contara con una guía de instalación que le facilitara a los alumnos la realización de este tipo de prácticas.

¿COMO SE DESARROLLA LA IDEA?

Para lograr realizar este prototipo, empezamos por encuestar a varias empresas, para consultar que tipo de herramientas utilizan para la gestión de
los equipos de red, dentro de las compañías visitadas están Digicel El Salvador.
Como resultado de dicha investigación obtuvimos un listado generalizado de varias herramientas que se encuentran en este ambiente de gestión de redes.
Luego se realizaron diferentes pruebas para lograr identificar cual de las diferentes herramientas era la mas completa y funcional.
Solarwinds fue la mejor elección, debido a que es un potente programa capaz de realizar diferentes operaciones, como lo es el monitoreo de diferentes recursos de hardware, alertas de errores y alta vigilancia de la red en general. Además es capaz de funcionar con diferentes plataformas de software como lo es Windows, Solaris, Unix, y Linux.
Es por eso que Solarwinds es capaz de controlar todos los recursos de software y de hardware de una manera centralizada así como también aplicaciones.

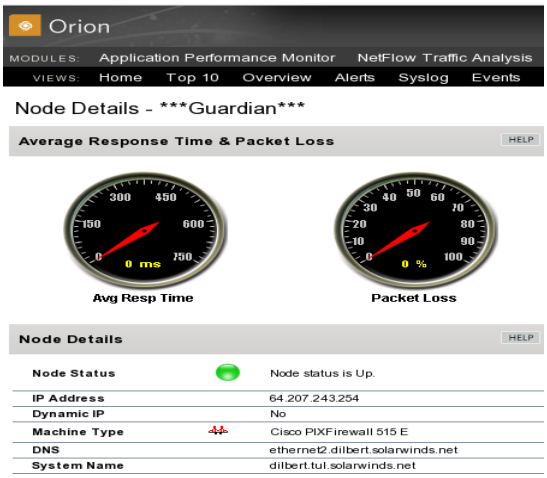


LOGROS QUE HEMOS OBTENIDO

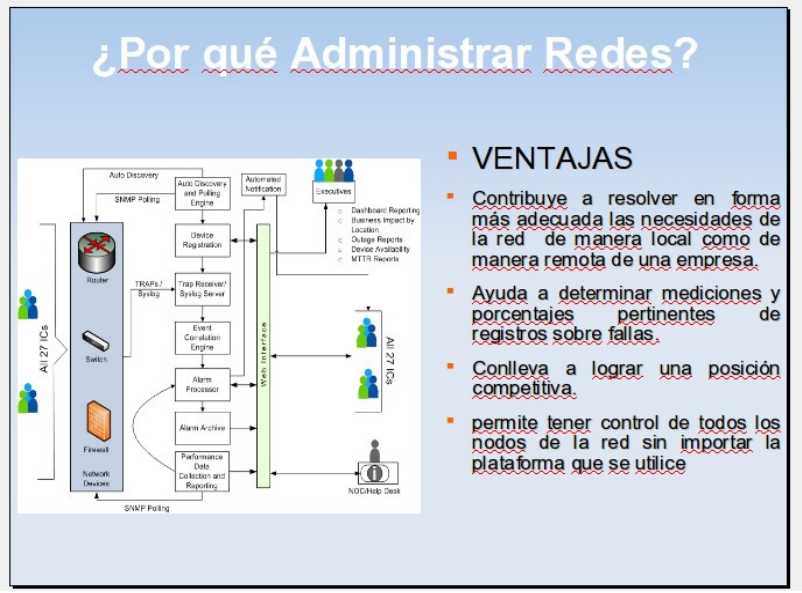
Con el desarrollo de este proyecto hemos logrado conocer mas sobre protocolos de gestión de redes como SNMP y de control remoto como RDP y XRDP. También hemos logrado integrar plataformas de sistemas operativos distintas para que de forma similar sean controladas con este software de gestión.
El producto ya se encuentra en su configuración de plena funcionalidad, para la cual ya estamos en el proceso de realizar la guía de utilización de ésta.

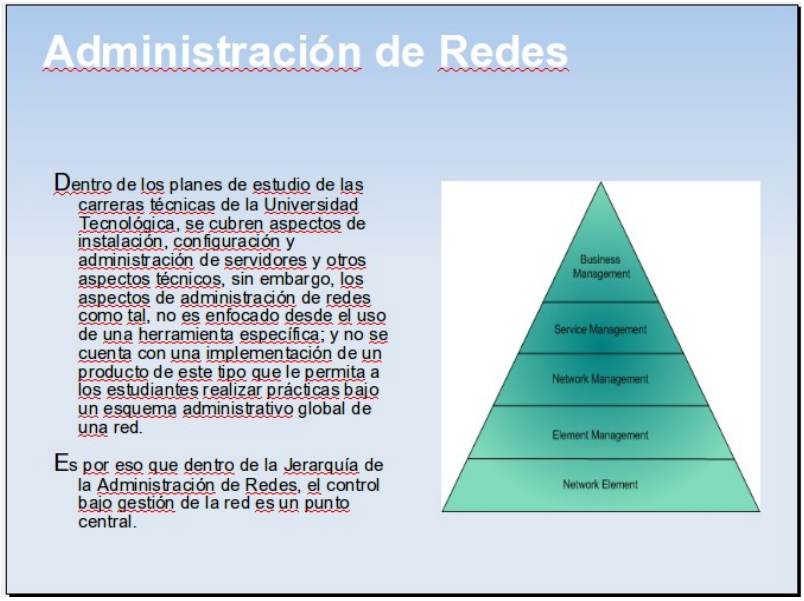
LO QUE SIGUE

Como parte de un compromiso de fraternidad hacia las nuevas generaciones de estudiantes, pretendemos dejar este proyecto implementado y documentado para que sea del provecho de todas las carreras técnicas de la Universidad Tecnológica, dejando así una herramienta que permita tener una visión más amplia sobre la administración centralizada de redes informáticas.



4.2 PRESENTACION





Ventajas

- Disponibilidad de su red directamente desde el navegador de red
- Monitorear desde 10 hasta más de 10.000 nodos
- Monitorea carga de la CPU, utilización de memoria, y espacio de disco disponible

Logros de la investigación

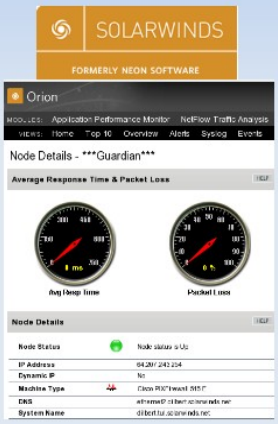
Dentro del proceso investigativo encontramos muy buenas herramientas para el control de la red, entre ellas:

Nagios®

CACTI

SOLARWINDS
FORMERLY NEON SOFTWARE

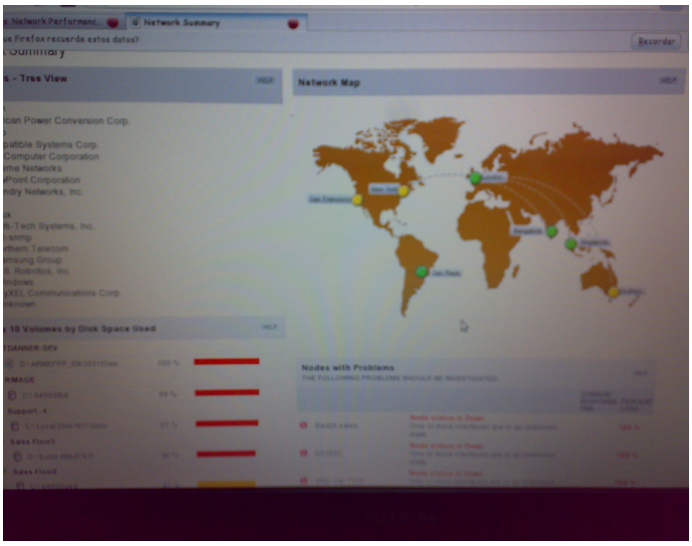
Nuestra propuesta



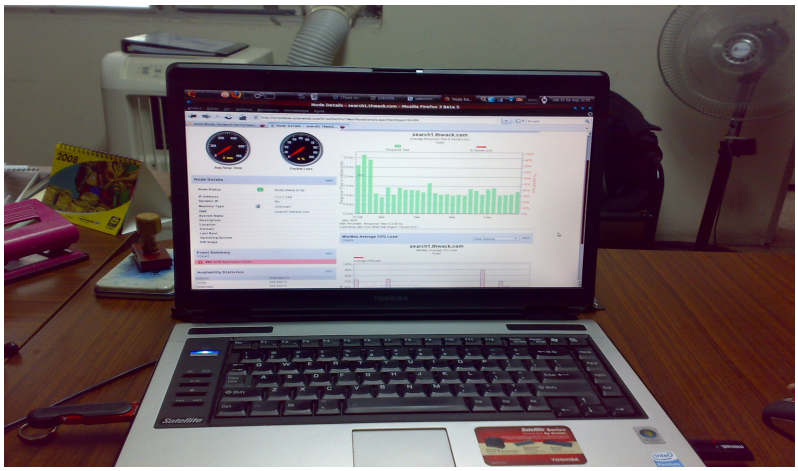
- Como parte de nuestra recomendación, ofrecemos SolarWinds como una de las herramientas mas completas, debido a que cuenta con muchas herramientas indispensables dentro del proceso de administración de Redes.

4.3 EVIDENCIA DEL PROTOTIPO

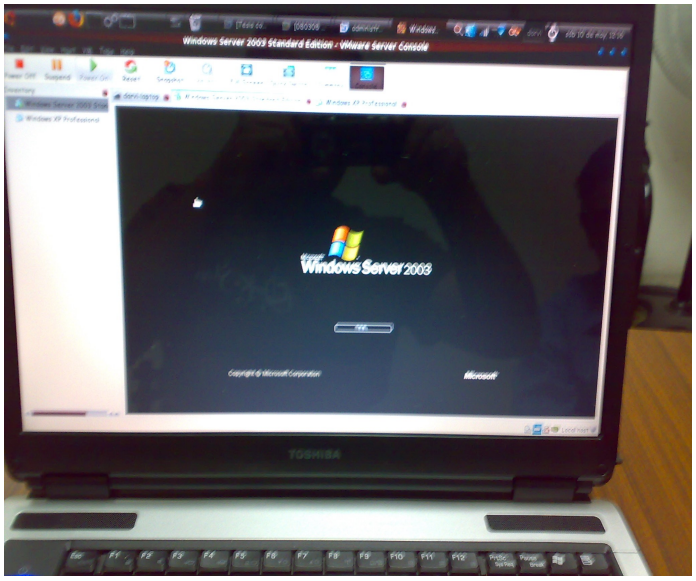
Interactuando con Solarwinds



Gestionando redes con Solardwinds



monitoreo de Rendimiento de CPU (Solarwinds Orion)



Iniciación de Windows 2003 server

CONCLUSIONES

- El contar con herramientas de gestión de redes, facilita la administraron de los servicios y equipos de la red.
- Es de gran importancia contar con historial del comportamiento de los equipos y aplicaciones en la red, para poder realizar predicciones de crecimiento o el control en el tiempo de fallas ocurridas, incluyendo el crecimiento de la carga de trabajo

- La inversión en un software comercial de gestión de redes es la alternativa mas segura y eficaz debido a el soporte y garantía del producto, que gerentes tecnología y administradores de redes deben considerar al momento de escoger una solución informática.
- La implementación de este tipo de herramientas debe de considerar por parte de los administradores de redes, la experiencia suficiente para brindar un buen soporte en la implementación de este producto.
- En base a la investigación realizada, Solarwinds es una aplicación de administración de desempeño, de fácil comprensión basada en la administración de fallas, disponibilidad y ancho de banda de la red que permite a los usuarios ver las estadísticas en tiempo real y la

disponibilidad de su red directamente desde el navegador de red, estas son características validas en ambientes críticos donde es necesario una rápida respuesta de problemas dentro de la red.

- Es de gran importancia que la herramienta de gestión de red brinde una serie de reportes que permitan cubrir de una manera fácil y comprensiva el estado de la red y los equipos que están bajo monitoreo.

RECOMENDACIONES

- Debido al tipo de actividad de monitoreo constante, se sugiere que el equipo donde se instale la herramienta de control este dedicada a esta actividad, para evitar que se pierdan paquetes de gestión de los equipos que se monitorean.

- Existen muchas herramientas basadas en software libre que permiten realizar el monitoreo y gestión de equipos en la red, sin embargo, una desventaja es que no se cuenta con soporte técnico suficiente para enfrentar posibles problemas que puedan sucitarse, es por esto que sugerimos para este tipo de finalidad, que la herramienta tenga un

soporte comercial bien establecido

- Es de gran importancia definir esquemas de seguridad para las comunidades basadas en SNMP para evitar que cualquier otro equipo pueda obtener información sobre el rendimiento y operación de los equipos.

BIBLIOGRAFÍA

Negus Christopher,Caen François *Ubuntu Linux toolbox 1000+ Commands for Ubuntu and Debian Power Users*. Primera Edición, Crosspoint Boulevard Indianapolis, Wiley Publishing, 2007. 363 pag.

Fundación Wikipedia [en línea] *Simple Network Management Protocol.* Última modificación : 3 de Julio de 2008. [consulta: 15 de junio de 2008] Wikipedia España, Comunidad GNU Española.
http://es.wikipedia.org/wiki/SNMP

Robert Waldie [en línea]: *Poptop the linux VPN server. Server and VPN client.* Última modificación: 19 de Abril de 2006. [consulta: 14 de Junio de 2008] Comunidad GNU linux.
http://poptop.sourceforge.net/dox/

Solard Winds Inc. [en línea].*Solar Winds Orion simple Network Manager*. Última modificación: Julio de 2008. [consulta: 21 de Abril de 2008]. http://www.solarwinds.com

Nagios LLC. [en línea]. *Nagios Enterprise*. Última modificación: 19 de Mayo de 2008. [consulta: 19 de Junio de 2008]. Nagios Network Manager.
http://www.nagios.org

ANEXOS

Implementacion de un sistema PBX que brinde las herramientas necesarias a la UTEC como apoyo al diplomado de call center

ENUNCIADO DEL PROBLEMA: ¿Cómo logrará la Universidad Tecnológica de El Salvador brindar a los estudiantes un laboratorio de de call center utilizando herramientas que sean flexibles de implementar y administrar ajo un entorno de licenciamiento gratuito?

ANEXO I

OBJETIVO GENERAL: Investigar herramientas para la administración y gestión de redes que permita que de forma efectiva y segura, la fácil administración de los recursos en la red.	**OBJETIVO ESPECIFICO 1**: Instalar una herramienta que será propuesta como la mejor alternativa para administrar redes de forma remota.	**ALCANCE 1:** Controlar y gestionar de manera remota mediante una herramienta de control y de administración de redes de forma sencilla, fácil, y funcional desde una ubicación centralizada.	**Marco teorico**
	OBJETIVO ESPECIFICO 2: Desarrollar una guía para implementar una herramienta que permita administrar una red de forma centralizada	**ALCANCE 2:** Elaborar un manual de instalación y configuración para la utilización de la aplicación Solarwinds.	
	OBJETIVO ESPECIFICO 3: Proponer una alternativa de conectividad remota para poder administrar a través de una herramienta los servidores de una red local.	**ALCANCE 3:** Implementar una alternativa de conectividad que sea segura y de fácil uso para poder administrar remotamente la red de la empresa.	

Producto 1: Dejar en operación un servidor con solarwinds que brinde servicios de administracion y monitoreo de la red	Proyecto tematico	Presupuesto	Oferta Economica
Producto 2: Entregar un manual de instalacion sobre Solarwinds orion y Ubuntu server .			
Producto 3: Habilitar un servidor de VPN con los servicios de Webmin con ubuntu server para la conectividad de los laboratorios de la utec.			

Producto 2:	Dejar en operación un servidor de Trixb

ɔx que opere con un número mínimo de dos extensiones para efectos demostrativos.

ubuntu

Ubuntu Server Edition 8.04 LTS

A rock solid opportunity for your business

Ubuntu Server Edition is changing the server market for businesses by delivering the best of free software on a stable, fully supported and secure platform. Ubuntu can now be found in hundreds of businesses across the world delivering key services reliably, predictably and economically.

Ubuntu Server Edition is becoming the backbone of many of the services that a typical business needs to run. With no license fees, an expanding ecosystem, minimal maintenance and a growing community of peers and references, Ubuntu Server Edition is making many businesses reconsider how they use Linux in their organisations.

Ubuntu users can enjoy outstanding performance, security and reliabilty:

- easily integrates into your existing networks
- provides a low total cost of ownership
- offers multiple life cycle scenarios for you to choose
- delivers free lifelong maintenance
- is backed by our world class support

Packed with features

Ubuntu Server Edition is loaded with features to simplify, optimise and secure your servers. The standard services listed over the page can be set-up during installation, meaning you can be up and running in minutes. These services require limited maintenance so once you've set it, you can forget it. Additionally, there are hundreds of other services and applications you can install to cover every server requirement your business has.

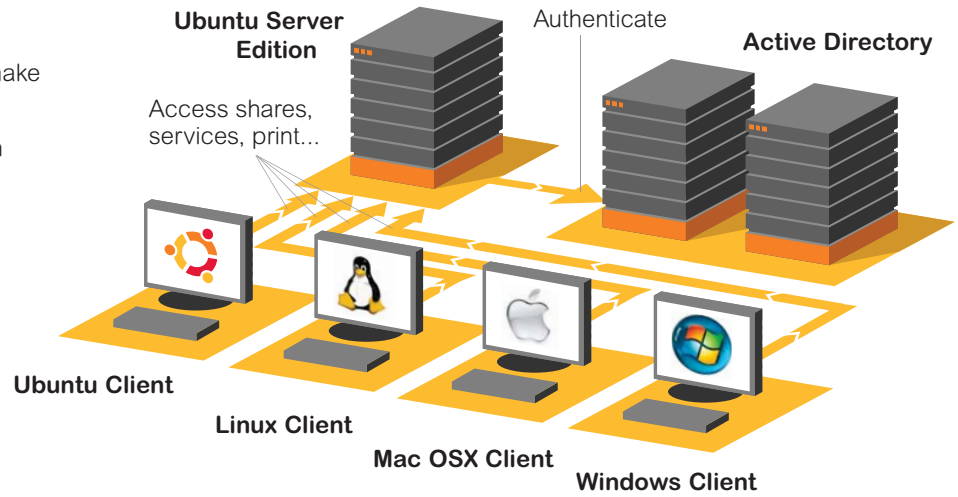
> "We replaced the proprietary Unix technology. The PC servers running Ubuntu cost a fraction of the old hardware cost."
>
> Ken Simon,
> Oakland University

Feature	Ubuntu Server Edition
Kernel	Uses a specifically tuned kernel to optimise your hardware and to handle all the most common server workloads. Also tuned specifically for virtualization where Ubuntu operates as an excellent hypervisor.
Mail server	Has all the features needed to provide e-mail services, whether acting as a connector to the Internet with Postfix, or as a central storage for users to access their e-mail with Dovecot. It also supports a range of content checkers to keep your organisation spam and virus free.
File and print server	Makes sharing files across multiple systems with Samba easy. CUPS shares printers across networks and minimises printer recognition issues.
Web application server	Serves dynamic web pages using your favourite tools including PHP, Perl, Python, Apache, MySQL or PostgreSQL with more options supported by vendors and the community, such as Java and Ruby.
Security	Offers great security for your business with it's easy to administer, but fine-grained security procedures. From kernel hardening to access control and years of free updates, Ubuntu Server will ace any security audit.
Authentication integration	Integrates easily with Windows, MacOSX, Unix and Linux. Also comes with Likewise Open and LDAP connectors to easily integrate with your current user management system, allowing your clients to seamlessly authenticate.
Automated deployment	Includes network & CD deployment, unattended installation, controlled installation, pre and post installation scripting, easy configuration GUI, automated updates and Landscape (Ubuntu systems management) integration.
Ubuntu Server Edition JeOS	Allows you to build virtual appliances. Configured to be as low footprint as possible, it allows you to run more appliances per server to maximise system usage.
Network infrastructure	Provides a range of network infrastructure services, including DNS with Bind 9, DHCP for easy network configuration and VPN's with OpenVPN. Additionally, includes FreeRadius, monitoring through Nagios or Munin and backup solutions with Bacula or BackupPC.

The benefits of switching to Ubuntu Server Edition

Ubuntu Server Edition is different. We make the same version available to everyone and we provide updates for the duration of its life cycle. We also focus on building it in a way that benefits real world administrators so that they can succeed in running the IT backbone of businesses.

Figure 1 – Seamless authentication integration



Services are simple to deploy

Ubuntu adds ease of use and efficiency, with a typical deployment taking just minutes for a fully secured and configured deployment of standard services. Today there is an array of vital services that can be deployed in this was including mail, web, DNS, file serving or database management. LAMP (Linux, Apache, MySQL and PHP) is also available at set-up.

This simplicity is because Ubuntu Server Edition takes a different approach to how it delivers packages. The basic configuration and integration work is done before installation so that the user only needs to select which option they want.

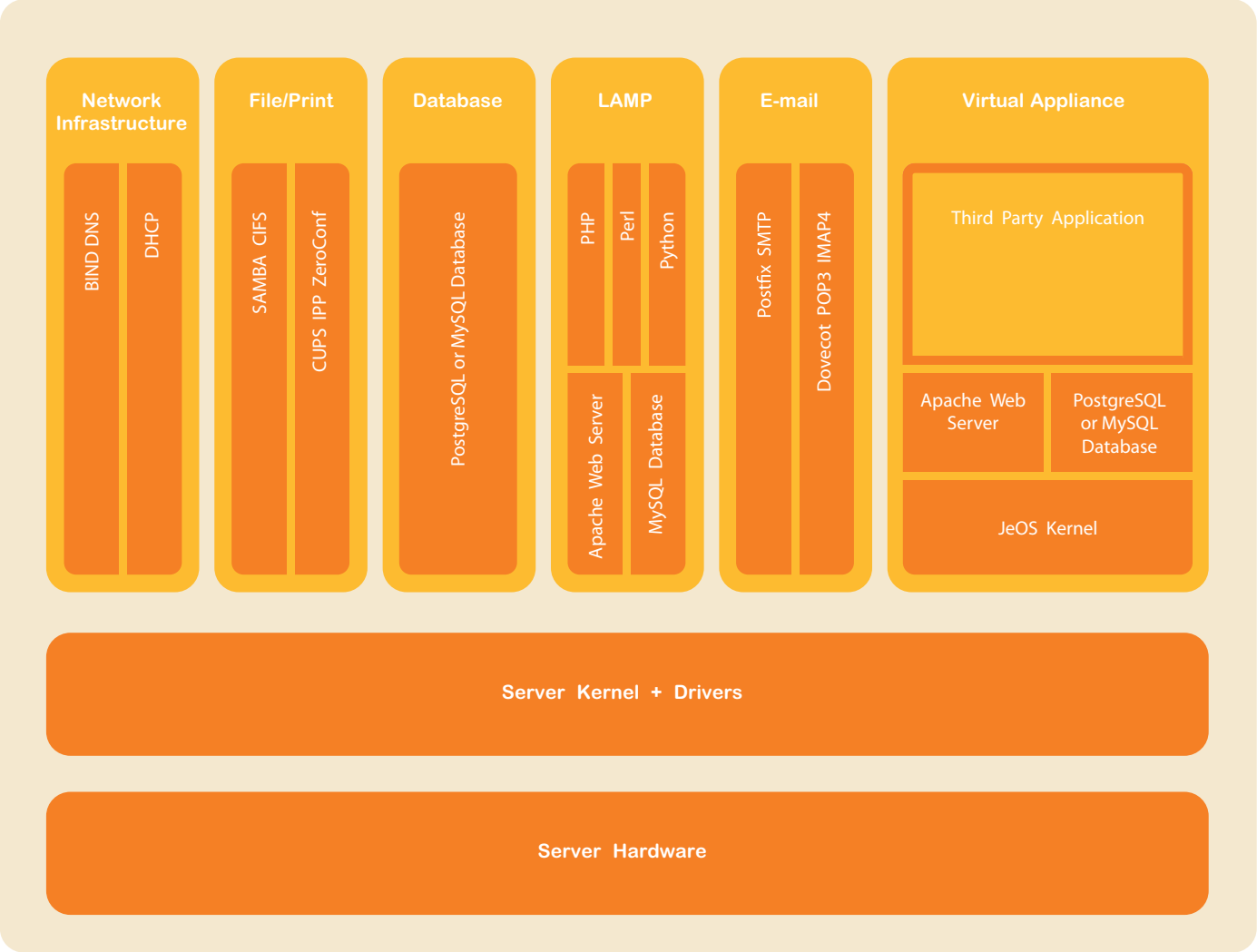


Figure 2 – A sample server configuration that can be set-up easily with Ubuntu Server Edition

Packages are straight forward to deploy and manage

We recognise that the administration and upgrade costs are another significant part of IT business spending. Therefore, we've made our server as easy to maintain as possible, which means that you can set it up and then forget about it.

- **The Debian packaging system** handles package files and configuration, allows for tight integration of different packages, permits updates of running services and provides excellent dependency control.
- **APT (Advanced Packaging Tool) management system** allows you to get fast and reliable automated update mechanisms that you can control fully, and it covers not only the operating system but all of the open source packages that you install on top of it. Administrators can easily learn how to package any program and publish them in a private repository, so they manage the system as one unique component.
- **Third party software** packages that are added from the partner repository get updated at the same time.
- **Automated deployments** save you time. Deploying new systems is time consuming and a repetitive process that can be fully automated to easily provision a new server in the most complex setups. The flexibility of the Debian installer allows fast network deployments or creation of custom CDs, including any special configuration that may be required.

CANONICAL

Lower your cost of ownership

Ubuntu Server Edition is free, and always will be. There is no 'for pay' edition that contains extras. We know that license fees are only the starting point in making a TCO argument in your business, therefore, consider the merits of Ubuntu Server Edition:

✔ **Easy to manage** – installation, startup, shutdown, service initialisation and package management.

✔ **Built for purpose** – no bloatware and no extraneous applications clogging up what you really want to do–run the services that run your business.

✔ **The platform for open and free computing** – take advantage of the fantastic array of open source server applications to increase the savings for your organisation.

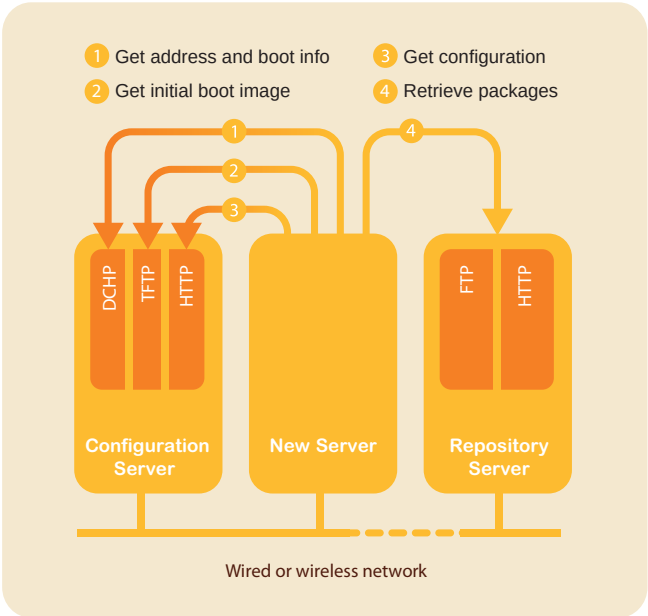
✔ **Simple to upgrade** – get the latest and greatest upgrades every 6 months or stay for the longer term on a single platform in the knowledge that we will ease the upgrade path. It's long term confidence.

✔ **Simple to update** – Debian packaging and APT are recognised as the easiest, smoothest methods of introducing software to your server stack. They are pre-configured to ensure a smooth introduction.

✔ **The ideal 'green' solution** – whether it is virtualization maximising your server efficiency or simply running lean services across your network, Ubuntu is a great partner in the drive to improve efficiency.

✔ **Security** – the greatest risks to your business are eliminated. Continuous updates respond to the changing landscape of risk on an already hard to hack distribution.

Figure 3 – Automated deployment



Predictable life cycle and maintenance policy

Our product life cycle ensures that you can perform upgrades of your systems, in place, time after time, at the pace you choose, without compromising the work you have put in setting them up.

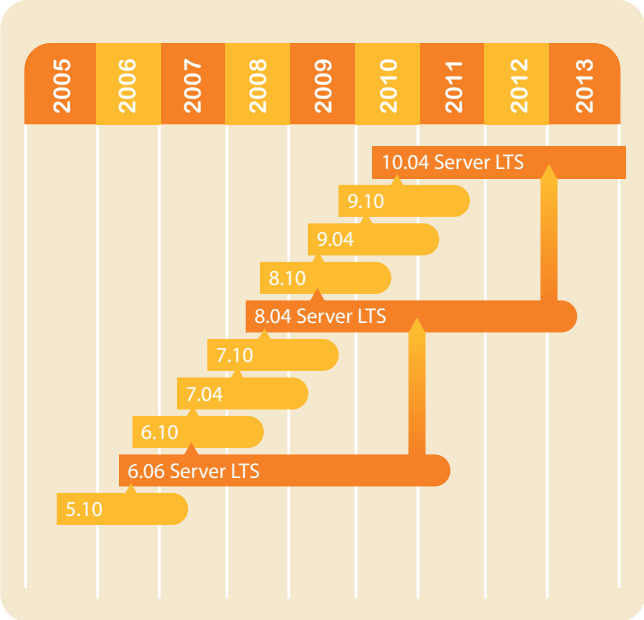


Figure 4 – Upgrade path

Ubuntu Server Edition has a dual release cycle

- Every 6 months a version is released that contains the latest packages and updates. This is maintained for 18 months from release with an upgrade path to the next 6 month release version.

- For greater robustness and easier planning, every 2 years a Long Term Support (LTS) version is released that is maintained for 5 years. This is a target platform for ISVs looking to build solutions on Ubuntu and also for larger deployments in need of a more stable release.

> “Ubuntu’s fine-grained package structure makes it an excellent choice for VMware virtualization. VMware and Canonical have worked to optimise Ubuntu 8.04 LTS for customers running VMware virtualization in data centres and on desktops, and Ubuntu’s Server JeOS is a compelling platform for ISVs building virtual appliances.”
>
> Dan Chu,
> Vice President of Emerging
> Products and Markets, VMware

Virtualization

Ubuntu Server Edition offers a variety of virtualization technologies for use as a host or guest operating system. There are open source and proprietary solutions to meet every need. KVM (Kernel Virtual Machine) is our open source virtualization solution, it’s efficient and comes with a suite of management tools. Additionally, we have established premier relationships with VMware and Parallels to offer a range of options to meet every requirement.

Storage Area Network

Ubuntu Server Edition brings the power of inexpensive shared storage to your servers. More and more organisations rely on the throughput of Gigabit Ethernet to build up their SAN (Storage Area Network) for data or virtual machine storage. Using relatively inexpensive hardware, the performance can be quite amazing.

Two key storage technologies feature in Ubuntu Server Edition: iSCSI and DRBD. They enable administrators to attach network storage to a server. These low level protocols can be used in conjunction with a variety of file systems and high availability capabilities to set-up scalable and robust server configurations.

Processor technologies

Ubuntu Server Edition is optimised for 32 or 64-bit multi-core processors. The Kernel team is working closely with Intel and AMD to implement the latest features the processors allow, and integrate the latest drivers the chipsets permit. This includes AMD’s V, Cool & Quiet and Hypertransport as well as Intel’s VT, IOAT and EIST.

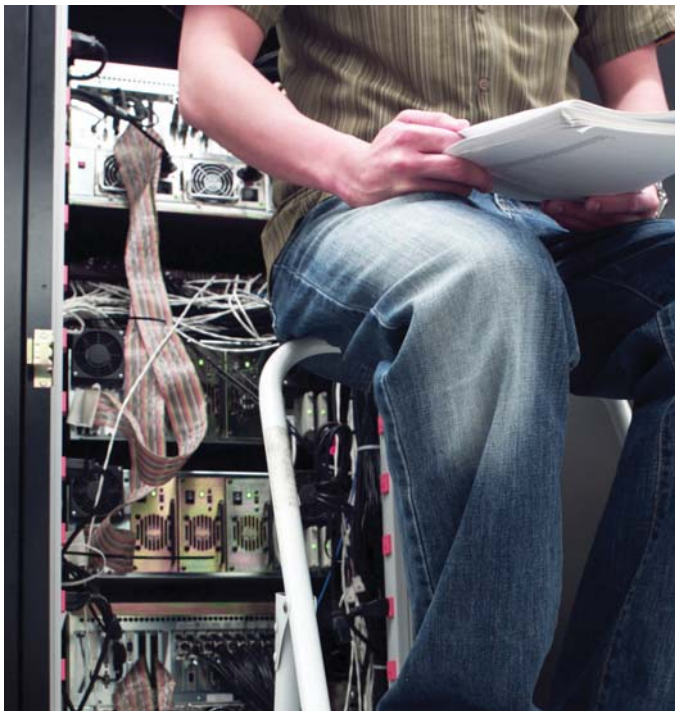
World class support from Canonical

Every business depends on their technology which is why you need Canonical’s professional support services behind you. Our focus is on providing exceptional support so that customers can deploy and manage their Ubuntu systems with confidence. Our support team has the knowledge and expertise to assist with the most difficult deployment and configuration problems.

Solving problems quickly and effectively is critical for effective IT management. As a support subscriber you will have immediate access to an expert who can answer your questions or help if something goes wrong. From simple configuration problems, to the resolving of mission critical bugs we’re there whenever you need us. For more information visit **www.canonical.com/services/support**

Canonical Landscape: System Management for Ubuntu

Deploying applications and security updates to multiple machines is a critical component in effective systems management. Landscape makes Ubuntu systems management simple, enabling you to manage multiple Ubuntu machines through a single web interface. Simply register a machine in Landscape and you can immediately start managing application, system and user resources.



CANONICAL

Technical specifications

Ubuntu Server Edition 8.04 LTS

Ubuntu Server Edition will run on Intel x86 based systems (including Intel Pentium, Intel Xeon and AMD Athlon) plus AMD64 and Intel64 based systems (including AMD Opteron and Intel EM64T Xeon). It requires a minimum of 256Mb of RAM.

The following is a selection of the common packages that are fully maintained in Ubuntu Server Edition.

Kernel	**Web**	**Database**
2.6.24	Apache 2	MySQL 5
KVM		PostgreSQL 8
E-mail	**Networking**	**Package management**
Dovecot	LTSP 5	Aptitude
Postfix 2.4	Samba 3	APT
Exim 4	OpenDAP 2.4	Dpkg
amavis-new	FreeRadius	
Languages	**Security**	**Clustering**
PHP 5.2.4	AppArmor	Ocfs 2
Perl 5.8	iptables	Lvm 2
Python 2.5	Uncomplicated Firewall	Gfs 2
C, C++	OpenVPN	DRBD 8
Ruby	Open SSH	open-iscsi

"Sun is committed to providing customers a choice of operating systems on our x64 servers. Sun has worked closely with Canonical since early 2006 and we continue to see growing interest in Ubuntu on Sun platforms."

Lisa Sieker,
Vice President of Systems Marketing, Sun Microsystems

For more information, please visit **www.ubuntu.com/server**

CANONICAL

Product Overview

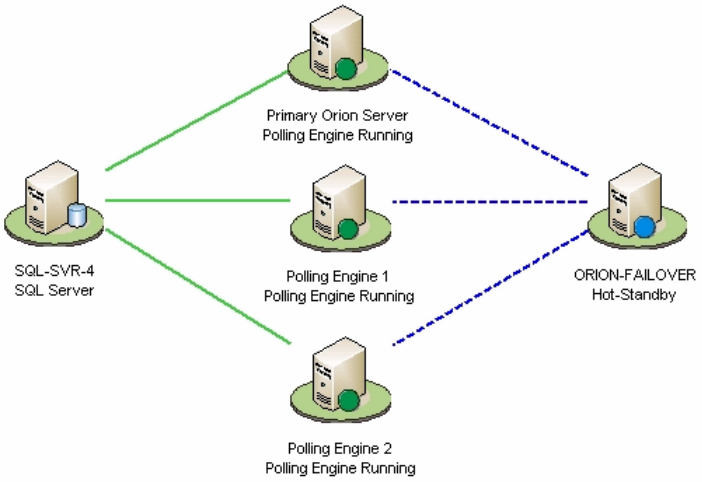
SolarWinds Premier Partner

Hot Standby Engine for Orion

The Orion Network Performance Monitor Hot Standby Engine will consistently check the Primary systems' ability to function and record availability and performance data. In the event of a failure, the Hot Standby Engine will automatically assume network-monitoring responsibility. When a failed Polling Engine returns to an operational state, the Hot Standby Engine will automatically return all monitoring tasks to the original Polling Engine.

Key Features

- Continuously checks the primary ORION system for activity
- Automatically takes over monitoring, statistic collection, and alerting if the primary system is down
- Automatically enters into "standby mode" when the Primary Orion server recovers
- Sends notifications for polling engine failures
- Offers 1-to-Many Failover Capability
- Runs on a separate server
- Uses your existing SQL database
- Includes a redundant website



Other Key Points

- Does not back up the Orion database (Use Database Manager or SQL Enterprise Manager to perform backups)
- Hot Standby Engine must be installed on a separate server
- The database MUST be on a separate server

Hot Standby Engine Pricing

SLX	£3,995	**SL250**	£1,140
SL2000	£2,795	**SL100**	£570
SL500	£1,750		

For volume, government, or educational pricing, please contact the SolarWinds Sales Department on +44 (0) 1403 791891 or mailto:sales@asl.co.uk

Also Available for Orion

Wireless Networks Management Pack £1,430

This management pack enhances Orion's ability to manage Wireless Access Point Routers and the associated wireless clients and sessions.

Application Monitor Management Pack £857

This management pack enhances Orion's ability to manage servers by monitoring the running processes, and tracking process status, memory, and processor utilization.

Network Services Management Pack Coming Soon!

This Management Pack will monitor network services such as HTTP, DNS, SNMP, SQL, etc., by opening the applicable TCP port and/or running a test transaction.

SOLARWINDS.NET
Network Management Software

ORION Network Performance Monitor

Web Enabled Network Management Software

ORION Application Monitor Management Pack

Requires a licensed version of Orion Network Performance Monitor

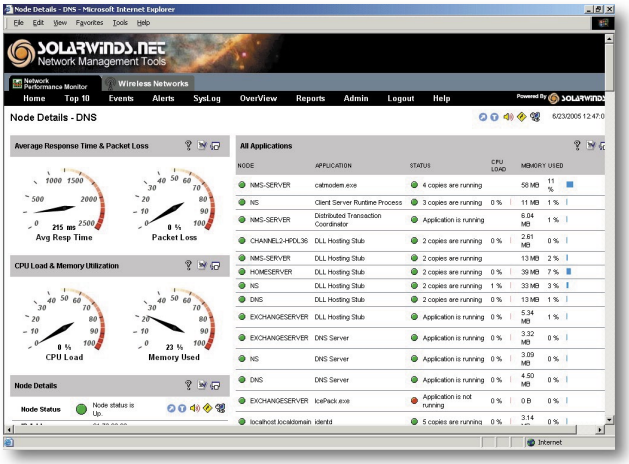
The ORION Application Monitor Management Pack extends the capability of the Orion Network Performance Monitor. This new management pack enhances Orion's ability to manage Windows, Unix and Linux servers that support the "Host Resource MIB" by monitoring the running processes on these machines and tracking process status, memory usage, and processor utilization.

The Application Monitor Management Pack installs on the same server as the Orion Network Performance Monitor and automatically integrates with the Orion polling engine, website, and database.

With a single license you can monitor the applications and processes on 5 servers or 5,000 servers. The license limitation is defined by the version of ORION installed. You only need one copy of the Application Monitor Management Pack for each of your Orion systems.

Features:

- Monitors processes running on Windows, Unix, and Linux Servers that support the Host Resource MIB
- Identifies failed and stopped processes on servers
- Records the number of concurrent running applications per server with associated Process ID's
- Tracks memory and CPU used by each monitored application
- Tracks memory used by each monitored application
- Displays the length of time each application has been running
- Does not require any agents to be installed on the monitored servers



SOLARWINDS.NET
Network Management Software

ORION Application Monitor Management Pack

The Application Monitoring Management Pack can be purchased to extend the monitoring capabilities of the ORION Network Performance Monitor. This management pack can be installed on any server which already has Orion installed. The Evaluation Version of the management pack can be installed on either a licensed or evaluation version of Orion. The following is an overview of the features and capabilities of the Application Monitoring Management Pack.

Monitor Services and Applications

Use the Application Monitor Management Pack to monitor services and applications running on Windows, Linux and Unix servers with the Host Resource MIB enabled. Orion's user customizable web views allow you to see which applications have stopped so that you can take immediate action. Orion's web views also provide you with the ability to group applications by type, server, status, and more.

Monitor Application Performance and Resource Usage

You can use the Application Monitor Management Pack to monitor the processor and memory usage of each application and service running on a server. This feature provides you the capability to use Orion's Top 10 Reports Page to display the Top 10 applications and services by processor utilization and memory usage. The application may be running but it may also be consuming 100% of the CPU.

Advanced Server Monitoring

Orion enables you to monitor your Windows, Linux and Unix servers for availability, response time, packet loss, traffic, errors, CPU load, memory utilization, available disk space, and more. Now, with the Application Monitor Management Pack you can drill down on a server that is experiencing high CPU load or memory utilization to see which application or service is causing the problem.

Application and Service Trending

Orion's historical graphs and reports allow you to watch for trends in application and service performance based on processor load and memory utilization. You can compare processor performance this month with last month or with this month last year.

System Requirements:
Pentium IV 1 Ghz
1 GB RAM
20 GB Hard Drive
Network Card

Windows 2000 Server or
Windows 2003

Includes:
Microsoft SQL Server 2000 (MSDE)

Download a Free
30 Day Evaluation
http://www.asl-orion.co.uk

SOLARWINDS.NET
Network Management Software

www.asl-orion.co.uk
Sales@asl.co.uk
phone:+44 (0) 1403 791891

SolarWinds ORION

Network Performance Monitor

Web Enabled Network Management Software

The Orion Network Performance Monitor

NPM provides access to real-time and historical **Performance Monitoring** and **Fault Management** directly from a **web browser.**

Instant Results

The auto-discovery and auto-configuration features of Orion enable the software to be installed and operational in less than an hour.

Reduced Downtime

The comprehensive **alert engine** and **event monitor** help identify network problems, keeping outages and downtime to a minimum. Orion alerts via: e-mail, pager, SNMP trap, text-to-speech, Syslog messages and more.

Orion Monitors

- Availability
- Network Latency
- Bandwidth Utilisation
- Interface Errors and Discards
- CPU and Memory Utilisation
- Volume Usage
- Node, Interface and Volume Status
- Buffer Usage and Errors

Maximise ROI

Most companies see a Return On Investment from Orion within 60-90 days.

Fully Customisable

The web-based vies can be customised to meet the needs of small companies, large enterprises and service providers. Views are fully customisable and web accounts can be limited based upon department, geographic area, customer ID or any of hundreds of sets of criteria.

Topology Based Views

Orion's web-enabled maps provide a real-time pictorial status of the network topology with the ability to click and drill into regions, departments and devices.

Advanced Reporting

The reporting feature aids in the analysis of network trends, capacity planning and provides instant access to availability, performance and utilisation statistics.

Scalable

Orion is friendly enough for even the smallest networks but powerful enough to manage the world's largest, most complex multi-vendor networks.

New Features:

Enhanced System Manager
Improved Polling Engine
New Type-Specific Node Details View
Remote Desktop Integration
Syslog Server
Support for Orion Management Packs

NEW: Orion Management Packs:

Wireless Network Management Pack:
Allows Customers to monitor their Cisco and Avaya Wireless Access Points and any WAP with support for the 802.11 MIB

Application Monitoring Management Pack:
Allows Customers to monitor the applications running on a server.

(must have Orion V7.8 with current support)

Download a Free
30 Day Evaluation
http://www.asl-orion.co.uk

System Requirements::
Pentium III 1 Ghz
1 GB RAM
20 GB Hard Drive
Network Card
Support for Windows 2003 Server, Windows XP Professional and Windows 2000

ASL™
Analyser Sales Limited
Shiprods Farm, Bashurst Hill, Slinfold,
West Sussex RH13 0PD United Kingdom
Tel: +44(0)1403 791891 Fax:+44(0)1403 791892
www.asl.co.uk

AUTORES DEL DOCUMENTO

- DARVI ALAN PEREZ ASCENCIO darvi1@hotmail.com
- RICARDO ERNESTO LEIVA soporte_1980@yahoo.es
- ROBERTO ANTONIO SUARES rsuarez@superselectos.com.sv