ASIGNATURA: Int. De tecnologías WAN

TEMA: Resumen Capitulo 6

DOCENTE: Juan Alberto Vivas Burgos

ESTUDIANTE: Alex Ricardo Puc Kumul

CARRERA: Ingeniería informática

Fecha de entrega: 29 de octubre del 2019

El trabajo a distancia significa trabajar lejos de un lugar de trabajo tradicional, a menudo desde una oficina doméstica. Los motivos para la elección del trabajo a distancia son variados e incluyen todo, desde la conveniencia personal hasta las oportunidades que se les otorgan a los empleados con lesiones o discapacidades de seguir trabajando durante los períodos de convalecencia.

El trabajo a distancia es un término amplio que hace referencia a realizar un trabajo mediante la conexión al lugar de trabajo desde una ubicación remota, con la ayuda de las telecomunicaciones. El trabajo a distancia eficaz es posible debido a conexiones de Internet de banda ancha, redes privadas virtuales (VPN) y tecnologías más avanzadas, incluidas Voz sobre IP (VoIP) y videoconferencias. El trabajo a distancia permite ahorrar dinero que de otro modo se gasta en viajes, infraestructura y soporte de instalaciones.

Las empresas modernas emplean a quienes no pueden trasladarse al trabajo todos los días o para quienes es más práctico trabajar desde una oficina doméstica. Estas personas, denominadas trabajadores a distancia, deben conectarse a la red de la empresa para poder trabajar desde sus oficinas domésticas.

Cada vez más empresas consideran beneficioso tener trabajadores a distancia. Con los avances en las tecnologías de conexiones de banda ancha e inalámbricas, el trabajo lejos de la oficina ya no presenta los mismos desafíos que en el pasado. Los empleados pueden trabajar de manera remota casi como si estuvieran en el despacho o la oficina de al lado. Las organizaciones pueden distribuir de manera rentable aplicaciones de datos, voz, video y en tiempo real a través de una conexión de red común que alcance a todos los empleados, sin importar cuán lejos o separados estén.

Las ventajas del trabajo a distancia se extienden mucho más allá de la habilidad de las empresas para obtener ganancias. El trabajo a distancia afecta la estructura social de las sociedades y puede tener efectos positivos en el medioambiente.

Cada vez más empresas consideran beneficioso tener trabajadores a distancia. Con los avances en las tecnologías de conexiones de banda ancha e inalámbricas, el trabajo lejos de la oficina ya no presenta los mismos desafíos que en el pasado. Los empleados pueden trabajar de manera remota casi como si estuvieran en el despacho o la oficina de al lado. Las organizaciones pueden distribuir de manera rentable aplicaciones de datos, voz, video y en tiempo real a través de una conexión de red común que alcance a todos los empleados, sin importar cuán lejos o separados estén.

Las ventajas del trabajo a distancia se extienden mucho más allá de la habilidad de las empresas para obtener ganancias. El trabajo a distancia afecta la estructura social de las sociedades y puede tener efectos positivos en el medioambiente.

Para conectarse efectivamente a las redes de la organización, los trabajadores a distancia necesitan dos conjuntos de componentes clave: componentes de la oficina doméstica y componentes corporativos. La opción de incorporar componentes de telefonía IP se está volviendo más común debido a que los proveedores extienden los servicios de banda ancha a más áreas. Pronto, los componentes de voz sobre IP (VoIP) y videoconferencias serán parte esperada de las herramientas de los trabajadores a distancia.

En general, la provisión de asistencia técnica para VoIP y videoconferencia requiere actualizaciones de estos componentes. Los routers necesitan la funcionalidad de calidad de servicio (QoS). La calidad de servicio se refiere a la capacidad de una red de proporcionar un mejor servicio para el tráfico de la red seleccionado, como lo requieren las aplicaciones de voz y video. El análisis detallado de la calidad de servicio (QoS) no se encuentra dentro del alcance de este curso.

VPN encriptado que conecta al trabajador a distancia con la red corporativa. Éste es el centro de las conexiones seguras y confiables del trabajador a distancia. La VPN es una red privada de datos que usa la infraestructura pública de telecomunicaciones. La seguridad de la VPN mantiene la privacidad mediante un protocolo de tunneling y procedimientos de seguridad.

Los trabajadores a distancia, a menudo, usan distintas aplicaciones (por ejemplo, correo electrónico, aplicaciones Web, aplicaciones críticas, colaboración en tiempo real, voz, video y videoconferencias) que requieren una conexión de un ancho de banda elevado. La elección de la tecnología de red de acceso y la necesidad de garantizar el ancho de banda adecuado son las primeras consideraciones que deben tenerse en cuenta cuando se conecta a los trabajadores a distancia.

El cable residencial, DSL y el acceso inalámbrico de banda ancha son tres opciones que proporcionan un ancho de banda elevado a los trabajadores a distancia. El ancho de banda bajo proporcionado por una conexión dial-up por módem no es suficiente, aunque resulta útil para el acceso móvil cuando se está de viaje. Una conexión dial-up por módem sólo debe considerarse cuando no hay otras opciones disponibles.

Para acceder a Internet, los trabajadores a distancia necesitan una conexión con un ISP. Los ISP ofrecen varias opciones de conexión. Los métodos principales de conexión que utilizan los usuarios domésticos y de pequeñas empresas son los siguientes:

- **Acceso dial-up:** opción económica que utiliza cualquier línea telefónica y un módem. Para conectarse al ISP, el usuario llama al número telefónico de acceso del ISP. Dial-up es la opción más lenta de conexión y, generalmente, los trabajadores móviles la utilizan en zonas donde no están disponibles opciones de conexión de mayor velocidad.
- **DSL:** generalmente, es más costoso que el dial-up, pero ofrece una conexión más rápida. El DSL también utiliza líneas telefónicas, pero a diferencia del acceso dial-up, el DSL proporciona una conexión continua a Internet. La opción de DSL emplea un módem especial de alta velocidad que separa la señal de DSL de la señal telefónica y proporciona una conexión Ethernet a una computadora host o LAN.
- **Módem por cable:** los proveedores del servicio de televisión por cable ofrecen esta opción. La señal de Internet es transportada en el mismo cable coaxial que suministra televisión por cable. Un módem por cable especial separa la señal de Internet de las otras señales transportadas en el cable y proporciona una conexión Ethernet a una computadora host o LAN.
- **Satélite:** los proveedores del servicio de satélite ofrecen esta opción. La computadora se conecta a través de Ethernet a un módem satelital que transmite señales de radio al punto de presencia (POP) más cercano dentro de la red satelital.

El acceso a Internet a través de una red de cable es una opción frecuente usada por los trabajadores a distancia para acceder a la red empresarial. El sistema de cable usa un cable coaxial que transporta las señales de radiofrecuencia (RF) a través de la red. El cable coaxial es el medio principal usado para construir sistemas de televisión por cable.

La mayor parte de los operadores de cable usan antenas parabólicas para recopilar señales televisivas. Los primeros sistemas eran unidireccionales, con varios amplificadores ubicados en series a lo largo de la red para compensar la pérdida de la señal. Estos sistemas usaban conexiones intermedias para conectar las señales de video del tronco principal a los hogares de los abonados, a través de cables de derivación.

Los sistemas de cable modernos proporcionan una comunicación bidireccional entre los abonados y el operador de cable. Los operadores de cable ofrecen ahora servicios de telecomunicaciones avanzados a los clientes que incluyen acceso a Internet de alta velocidad, televisión digital por cable y servicio de telefonía residencial. Los operadores de cable en general implementan redes de fibra coaxial híbrida (HFC) para permitir la transmisión de datos a alta velocidad a los módems por cable ubicados en las pequeñas oficinas y oficinas domésticas.

DSL

DSL es una forma de proveer conexiones de alta velocidad mediante cables de cobre instalados. En esta sección, analizamos DSL como una de las soluciones clave disponibles para el trabajador a distancia.

DSL asimétrica (ADSL) usa un rango de frecuencia de 20 kHz a 1 MHz aproximadamente. Por suerte, sólo se requieren cambios relativamente pequeños en la infraestructura existente de las empresas telefónicas para ofrecer velocidades de datos de ancho de banda elevado a los suscriptores. La figura muestra una representación de la asignación del espacio de ancho de banda en un cable de cobre para ADSL. El área de color azul identifica el rango de frecuencia usado por el servicio telefónico de grado de voz, el cual se denomina en general servicio telefónico analógico (POTS). Los demás espacios en colores representan el espacio de frecuencia usado por las señales DSL ascendentes y descendentes.

Existen dos tipos básicos de tecnología DSL: la asimétrica (ADSL) y la simétrica (SDSL). Todas las formas de servicio DSL se pueden clasificar como ADSL o SDSL y existen muchas variedades de cada tipo. ADSL brinda un mayor ancho de banda descendente al usuario que el ancho de banda de carga. SDSL ofrece la misma capacidad en ambas direcciones.

Los distintos tipos de DSL brindan diferentes anchos de banda, algunos con capacidades que exceden aquellas de la línea alquilada T1 o E1. La velocidad de transferencia depende de la longitud real del bucle local y del tipo y la condición de su cableado. Para obtener un servicio satisfactorio, el bucle debe ser menor a 5,5 kilómetros (3,5 millas).

Los proveedores de servicio implementan conexiones DSL en el último paso de una red telefónica local, lo que se denomina bucle local o última milla. Se instala la conexión entre un par de módems ubicados en cualquier extremo de un cable de cobre que se extiende entre el equipo local del cliente (CPE) y el multiplexor de acceso DSL (DSLAM). El DSLAM es el dispositivo ubicado en la oficina central (CO) del proveedor, que concentra las conexiones desde los distintos suscriptores DSL.

La mayor ventaja de ADSL es la habilidad de proporcionar servicios de datos junto con servicios de voz POTS.

Cuando el proveedor del servicio coloca voz analógica y ADSL en el mismo cable, divide el canal POTS desde el módem ADSL por medio de filtros o divisores de señal. Esta configuración garantiza el servicio telefónico normal sin interrupciones, aun si ocurre una falla en el ADSL. Cuando los filtros o divisores de señal están en su lugar, el usuario puede usar la línea de teléfono y la conexión ADSL al mismo tiempo, sin afectar ninguno de los servicios.

Las señales ADSL distorsionan la transmisión de voz y se dividen o filtran en las instalaciones del cliente. Hay dos maneras de separar ADSL de la voz en las instalaciones del cliente: mediante un microfiltro o un divisor de señal.

El acceso de banda ancha por ADSL o cable proporciona conexiones más rápidas a los trabajadores a distancia que el servicio dial-up; sin embargo, hasta hace poco, los equipos de las oficinas pequeñas y domésticas debían conectarse a un módem o router por un cable Cat 5 (Ethernet). Las conexiones de red inalámbricas, o Wi-Fi (del inglés, Wireless Fidelity), han mejorado esa situación no sólo para las oficinas pequeñas u oficinas domésticas, sino también en los campus empresariales.

Redes VPN y sus beneficios

nternet es una red IP de acceso público en todo el mundo. Debido a su amplia proliferación global, se ha convertido en una manera atractiva de interconectar sitios remotos. Sin embargo, el hecho de que sea una infraestructura pública conlleva riesgos de seguridad para las empresas y sus redes internas. Afortunadamente, la tecnología VPN permite que las organizaciones creen redes privadas en la infraestructura de Internet pública que mantienen la confidencialidad y la seguridad.

Las organizaciones usan las redes VPN para proporcionar una infraestructura WAN virtual que conecta sucursales, oficinas domésticas, oficinas de socios comerciales y trabajadores a distancia a toda la red corporativa o a parte de ella. Para que permanezca privado, el tráfico está encriptado. En vez de usar una conexión de Capa 2 exclusiva, como una línea alquilada, la VPN usa conexiones virtuales que se enrutan a través de Internet.

Características de los VPN seguras.

Confidencialidad de datos: La confidencialidad de datos, que es una función de diseño, tiene el objetivo de proteger los contenidos de los mensajes contra la intercepción de fuentes no autenticadas o no autorizadas. Las VPN logran esta confidencialidad mediante mecanismos de encapsulación y encriptación.

Integridad de datos: La integridad de datos garantiza que no se realicen cambios indebidos ni alteraciones en los datos mientras viajan desde el origen al destino. Generalmente, las VPN utilizan hashes para garantizar la integridad de los datos. El hash es como una checksum o un sello (pero más robusto) que garantiza que nadie haya leído el contenido. En el próximo tema se incluye la explicación de los hashes.

Autenticación: la autenticación garantiza que el mensaje provenga de un origen auténtico y se dirija a un destino auténtico. La identificación de usuarios brinda al usuario la seguridad de que la persona con quien se comunica es quien cree que es. Las VPN pueden utilizar contraseñas, certificados digitales, tarjetas inteligentes y biométricas para establecer la identidad de las partes ubicadas en el otro extremo de la red.

Protocolos de seguridad Ipsec.

El IPsec es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación. IPsec ingresa el mensaje necesario para proteger las comunicaciones VPN, pero se basa en algoritmos existentes. Existen dos protocolos de estructura Ipsec, que son:

Encabezado de autenticación (AH): se utiliza cuando no se requiere o no se permite la confidencialidad. AH proporciona la autenticación y la integridad de datos para paquetes IP intercambiados entre dos sistemas. Verifica que cualquier mensaje intercambiado de R1 a R3 no haya sido modificado en el camino. También verifica que el origen de los datos sea R1 o R2. AH no proporciona la confidencialidad de datos (encriptación) de los paquetes. AH Proporciona lo siguiente:

- Autenticación
- Integridad

Contenido de seguridad encapsulado (ESP): proporciona confidencialidad y autenticación mediante la encriptación del paquete IP. La encriptación del paquete IP oculta los datos y las identidades de origen y de destino. ESP autentica el paquete IP interno y el encabezado ESP. La autenticación proporciona autenticación del origen de datos e integridad de datos. Aunque tanto la encriptación como la autenticación son opcionales en ESP, debe seleccionar una como mínimo. ESP proporciona lo siguiente:

- Encriptación
- Autenticación
- Integridad