Red virtual privada (VPN)

Acceso remoto seguro a las máquinas mediante VPN

ÁMBITO

Con PLC y controladores de máquinas con puertos Ethernet compatibles con el protocolo TCP/IP es muy fácil acceder a estos dispositivos de forma remota. La tecnología empleada para ello se conoce habitualmente como Red Virtual Privada (VPN). Una conexión VPN garantiza la transferencia segura de datos de una red a otra o de un dispositivo a otro en una red compartida o pública, como Internet.

CONTENIDO

DOCUMENTO TÉCNICO

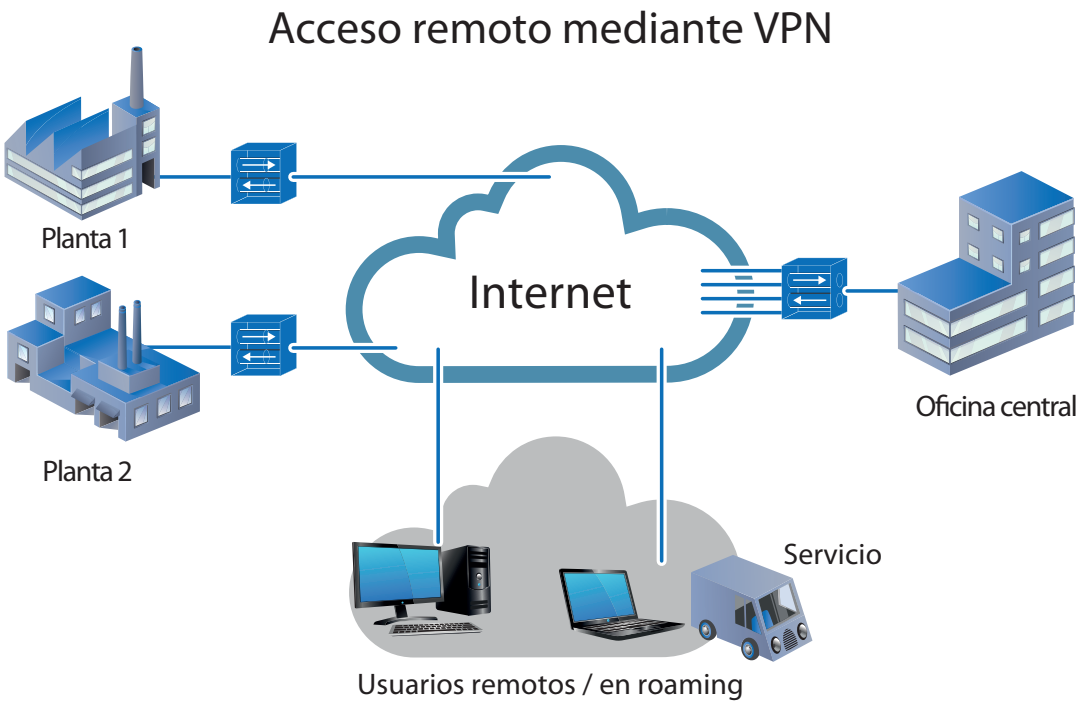
Resumen ejecutivo

Ventajas para la empresa

El uso del acceso remoto mediante VPN proporciona grandes beneficios tanto al fabricante de la maquinaria como al usuario final. El fabricante puede diagnosticar problemas de forma inmediata en la máquina, incluso antes de que se manifiesten; de esta forma puede informar al usuario para que puedan implementarse acciones preventivas o ayudarle a resolver la incidencia mediante asistencia remota. Además, el usuario final se beneficiará del acceso remoto, ya que el acceso a la máquina es sencillo y proporciona información en tiempo real sobre la producción.

El funcionamiento de las redes virtuales privadas permite realizar cualquier tipo de comunicación IP, incluida la comunicación con aquellos dispositivos que no disponen de una conexión Ethernet como un dispositivo serie mediante una conversión IP a serie. Este tipo de comunicación no tiene casi limitaciones y las posibilidades son prácticamente infinitas.

El hecho de disponer de acceso remoto a una máquina es prácticamente lo mismo que estar sentado al lado.



VPN establece una conexión entre dos sitios. La conexión está asegurada por el nombre de usuario y la contraseña, y los datos transferidos se cifran. Esto hace que sea muy poco probable que los usuarios ajenos puedan interferir en el funcionamiento de la máquina o acceder a los datos de producción. Una conexión VPN también se denomina túnel VPN, ya que lo que entra por un extremo sale por el otro sin ningún cambio.
Existen diferentes productos estándar para establecer una conexión entre diferentes sitios.
En este documento se proporciona una descripción general de los productos y tecnologías utilizados, su principio de funcionamiento y una explicación de la terminología.

Solución de alto nivel

Los modernos sistemas de control de máquinas pueden proporcionar una gran cantidad de información sobre el proceso que controlan; ya sean datos de producción o datos eléctricos y mecánicos sobre el estado de la máquina.

Por ejemplo, el controlador de la máquina registra y elabora informes sobre el consumo de energía de una unidad. Durante la fase de diseño de una máquina se calcula la carga de una unidad, mientras que los umbrales se definen durante la puesta en servicio. El controlador de la máquina controla el consumo de corriente de la unidad según el umbral y activa una alarma cuando la corriente excede ese umbral. También se puede establecer otro umbral como prealarma, que genera una advertencia cuando es necesario planificar tareas de mantenimiento o inspección en la unidad.

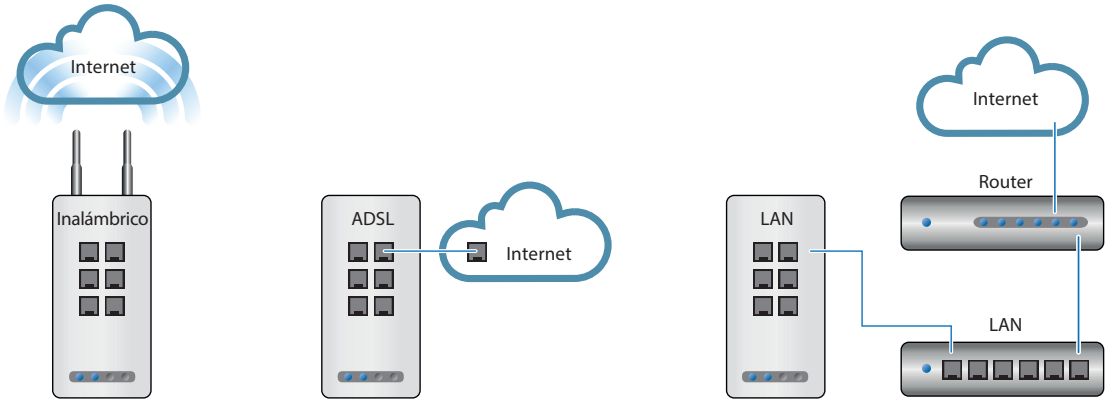
Esta información es importante para el usuario de la máquina para evitar paradas de producción no deseadas. Si el fabricante tiene un contrato de mantenimiento con el usuario final para evitar pérdidas como consecuencia de una parada de la producción, configurar una prealarma puede evitar costosas reparaciones.

El control de los tiempos de respuesta o vibraciones de la máquina puede detectar el desgaste de las piezas mecánicas. En este caso, el fabricante puede enviar piezas de repuesto de manera preventiva al usuario, de forma que las piezas se puedan sustituir durante la siguiente parada de mantenimiento planificada.
Como resultado, el usuario final se beneficia al reducirse la cantidad de averías y reparaciones de emergencia.

Formas de acceso

Con las tecnologías de comunicación actuales existen muchas posibilidades para crear una conexión con la máquina. Entre otras:

- Conexión inalámbrica mediante una conexión GPRS o UMTS.
- La máquina se conecta a la red local de la planta.
- Hay disponible una conexión a Internet por ADSL, cable, fibra o conexiones similares.

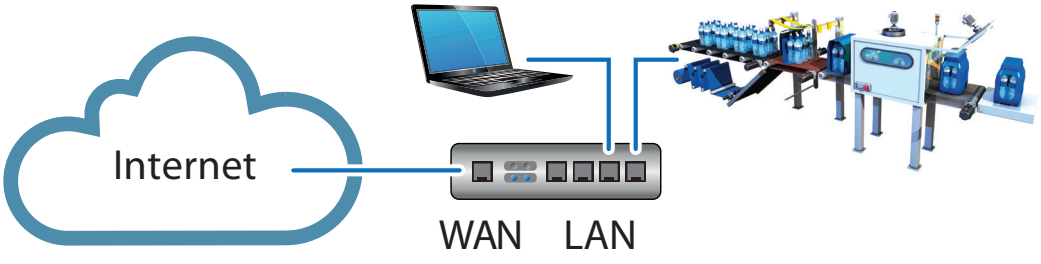


Conexión inalámbrica *ADSL / Cable* *Red local*

Con independencia del tipo de conexión que se use, los datos se pueden transferir directamente desde la máquina al fabricante. En este caso, hablamos de routers y se emplean para conectar la red local a una red mayor, que puede ser Internet o una red formada por varias plantas de producción.

Acceso remoto mediante VPN

La tecnología utilizada para el acceso remoto se denomina Red Virtual Privada (VPN).
Se trata de una conexión entre dos dispositivos que inician la conexión reconociéndose entre sí y, a continuación, se autentican y establecen un método de cifrado. Cuando se activa la conexión, ambos dispositivos pueden transferir datos de una forma segura y protegida contra intrusiones.

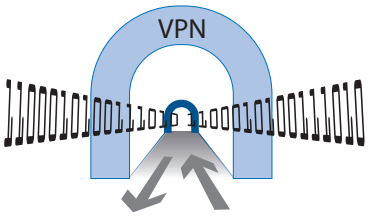


Desde el punto de vista del usuario, es como si estuviera sentado junto a la máquina. Sin embargo, puede que esa máquina esté ubicada literalmente en el otro extremo del mundo.

Imagine que ese dispositivo tiene un puerto WAN (Wide Area Network, red de área amplia) para conectarse a una red mayor o a Internet, y un par de puertos LAN (Local Area Network, red de área local) para crear una red local. Las dos redes LAN distantes se conectan y actúan como una sola a través de las funciones de enrutamiento. El dispositivo conectado al extremo LAN del router puede comunicarse con otros dispositivos en los otros extremos de LAN. Esto es de gran utilidad ya que es posible acceder a un controlador de la máquina desde el otro extremo. En lugar de un punto final (router) que es un dispositivo con puertos WAN y LAN también podría ser un PC que se conecta a la otra red.

Seguridad

El envío de datos a través de Internet u otras redes implica un riesgo para la seguridad. Por supuesto, es imprescindible evitar que un usuario pueda interceptar los datos enviados a través de la red y sabotear el sistema. VPN crea un túnel seguro en el sentido en que las comunicaciones se autentican cuando se abre la conexión y que los datos se transfieren cifrados. La autenticación puede basarse en nombre de usuario/contraseña, en claves precompartidas o en certificados (o una combinación de los tres métodos). Con frecuencia se utiliza un nombre de usuario junto con un certificado.



El cifrado puede ser sencillo o de muy alto nivel. Tenga en cuenta que el cifrado y descifrado de los datos requiere tiempo. Cuanto mayor sea el cifrado, más tiempo se tarda en preparar los datos y, por tanto, más lenta será la transferencia. Una solución para las instalaciones de alto nivel de cifrado puede ser utilizar un dispositivo con suficiente potencia de procesamiento para completar el cifrado/descifrado rápidamente. Los dispositivos más rápidos tienen con frecuencia un precio superior. No existe ningún método preciso para decidir el nivel de cifrado que se debe utilizar; depende del nivel de seguridad y de la velocidad de comunicación que se necesite.

Tipos de datos transferidos

En principio, es posible enviar cualquier tipo de datos IP a través de la conexión VPN. A continuación se enumeran algunos ejemplos prácticos:

- Alarmas y avisos de la máquina al OEM.
- Comunicación bidireccional entre la SCADA o interfaz remota y la máquina.
- Recepción o transmisión de información a y desde un servidor de bases de datos remoto (como Oracle o Microsoft).
- Nuevos programas de control cargados en la máquina para implementar modificaciones o actualizaciones.
- Control del estado para identificar averías en la máquina. Puede ser algo tan sencillo como comprobar si una señal del sensor se activa o programar que los sensores se deben volver a alinear.

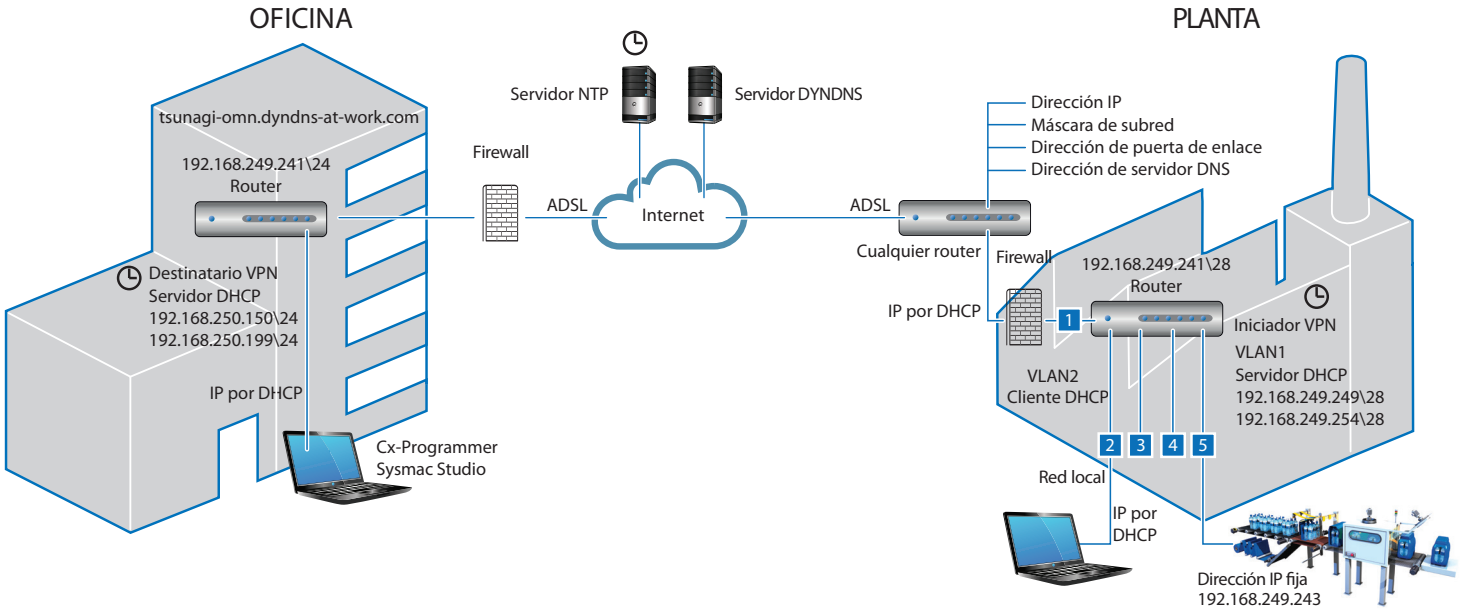
Cliente/servidor, iniciador/destinatario

Cada dispositivo tiene una función distinta en la configuración de la conexión VPN. Uno de los dispositivos actúa como iniciador o cliente de la conexión, mientras que el otro es el destinatario o servidor. El servidor espera al cliente para conectarse. La función de un servidor no es sólo servir a un cliente, sino a varios.
Los routers de las máquinas tienen la función de cliente y se conectan al servidor en las instalaciones del fabricante, que tiene todas sus máquinas en línea.

Las máquinas pueden informar sobre su estado de manera directa y continuada; de esta forma, el fabricante puede reaccionar inmediatamente ante cualquier evento. Y no sólo en caso de incidencias, sino también en caso de mantenimiento programado o si es necesario enviar repuestos de acuerdo con la información que envía cada máquina.

Detalles de la solución

En una red se suelen utilizar productos de distintos fabricantes. Sin embargo, estos dispositivos deben entenderse, por lo que es necesario estandarizar los protocolos.
En la tecnología VPN también hay un alto nivel de estandarización. No existe una VPN estándar sino varias: las dos principales son IPSec y OpenVPN (también denominada SSL).
Los productos y servicios disponibles más frecuentemente incluyen estos dos estándares. Gracias al uso de componentes COTS, cualquier usuario puede configurar su propia infraestructura VPN.



Caso práctico de VPN

La ilustración anterior es un ejemplo de un controlador de una máquina conectado a la red del fabricante. La ilustración muestra los componentes que se utilizan para configurar un túnel VPN entre dos sitios.
En el lado izquierdo encontramos la sede del fabricante de la máquina (servidor VPN). En la parte derecha está la red de una máquina instalada en una planta remota (cliente VPN). La red de la máquina está conectada por el túnel VPN a la red del fabricante, por lo que se dispone de acceso inmediato a la máquina.

La máquina está conectada a una red de la planta que tiene conexión a Internet. El router de la máquina está configurado para crear una red LAN local en la máquina y se conecta mediante uno de sus puertos (WAN) a Internet a través de la red de la planta.

Los servicios locales son:

- VLAN (Virtual Local Area Network, Red de área local) se utiliza para dividir los puertos Ethernet de los routers en dos redes diferentes. El tráfico no se puede pasar de una red a otra y viceversa. Una VLAN (la red local) tiene su propio rango de direcciones IP y es el punto final de la conexión VPN. La otra VLAN (WAN) es parte de la red de la planta y obtiene su dirección IP y otros parámetros de un servidor DHCP en la red. En la red de la planta, la máquina se representa como un único dispositivo con una sola dirección IP.
- El enrutamiento envía mensajes de una VLAN a otra según la dirección de destino. También detiene las emisiones y los mensajes de multidifusión de la red de la planta que entran a la red local de la máquina.
- El firewall detiene los ataques a la red de la planta. El firewall se puede abrir para que acepte determinados tipos de mensajes, si bien esta función depende totalmente de cada aplicación concreta.
- El servidor DHCP asigna las direcciones IP a los dispositivos de la red local. Normalmente, los dispositivos de control tienen direcciones IP fijas, pero puede suceder que un técnico de servicio conecte su portátil a esta red local, por lo que es recomendable que reciba la dirección IP asignada correcta.

La máquina forma parte de la red de la planta, por lo que no es posible acceder desde fuera de la planta. El router de la planta que se conecta a Internet dispone de un firewall y bloqueará todo el tráfico entrante. Por lo tanto, el router de la máquina tiene que ser el iniciador de la conexión VPN. Para establecer correctamente la conexión VPN, el iniciador VPN (el router de la máquina) debe tener la siguiente configuración.

- Sincronización de hora. Los procesos de negociación y cifrado también utilizan datos de fecha y hora. Tanto el iniciador como el destinatario deben tener la misma hora y fecha. La fecha exacta y la hora se obtienen de los denominados servidores horarios (servidores NTP). Un servidor horario puede estar ubicado en Internet o en la red de la planta. Un servidor horario garantiza que la fecha y la hora se establecen automáticamente y se ajustan regularmente.
- Servidor de nombre de dominio (DNS). Para que el iniciador de la VPN llegue al destinatario necesita saber su dirección en Internet. Sin embargo, las direcciones IP fijas de Internet son escasas y muy costosas, por lo que es más fácil tener un nombre de dominio. El servidor DNS asigna al dominio una dirección IP. El router sólo conoce el nombre (oficina.fabricante.com), pero le solicita al servidor DNS la dirección IP vinculada a este nombre para poder llegar al destinatario. Por eso no importa la frecuencia con que la dirección IP del servidor cambie; siempre es posible acceder a través de su nombre.

En el sitio del destinatario se deben configurar los siguientes elementos:

- Al igual que ocurre con el iniciador VPN, la hora del destinatario debe estar configurada correctamente. Puede utilizar el mismo servidor horario que el iniciador de VPN.
- El iniciador VPN busca el destinatario VPN por su nombre, por lo que el router debe indicar su nombre y dirección IP regularmente a un servidor DNS en Internet; este servicio DNS se denomina DNS dinámico. Algunas empresas ofrecen este servicio como DynDNS.
- La configuración de la conexión VPN del iniciador debe estar registrada en el destinatario.

Si se detecta una solicitud de conexión entrante, se comprueban sus credenciales y, si son correctas, la conexión se acepta y el túnel se abre. La red de la máquina ya está conectada a la red de la oficina y se pueden intercambiar datos directamente.

En el caso de las conexiones inalámbricas directas o cableadas, la conexión es algo más simple, pero básicamente es similar.

Tecnología de conexión

Cuando se crea un túnel VPN se debe establecer una conexión desde el cliente al servidor. En muchos casos, esta conexión se realiza a través de Internet. Existen varias formas para conectarse a Internet según la opción disponible en esa ubicación.
De manera general hay tres variantes: conexión mediante cable o inalámbrica, conexión directa o mediante una red local más grande.

Conexión inalámbrica

Hay ubicaciones en las que sólo es posible el acceso inalámbrico, por ejemplo en sitios remotos donde no hay conexión ADSL o de cable, pero sí es posible establecer la comunicación mediante una red móvil. Para acceder a esta red móvil se necesita una suscripción a un proveedor de servicios y una tarjeta SIM.

Existen diferentes tipos de comunicación inalámbrica de datos, pero las más conocidas son GPRS y UMTS. GPRS es una tecnología más antigua y con menos capacidad que UMTS. La tecnología UMTS ofrece velocidades de comunicación de megabits por segundo, mientras que el rendimiento de GPRS está limitado a unos cientos de kilobits por segundo.
Para garantizar la comunicación de datos en todo momento, GPRS funciona siempre que no es posible establecer una comunicación mediante UMTS. Tanto para UMTS como para GPRS el coste de la conexión se basa en la cantidad de datos transmitidos, no en el tiempo de conexión. Por lo tanto, la conexión puede estar funcionando todo el tiempo.

Conexión cableada, conectada directamente a Internet

El router de la máquina se conecta directamente a Internet mediante una conexión ADSL, por cable o de fibra. Un proveedor de servicios local instala la conexión y es posible acceder a Internet desde la máquina.

Conexión cableada a una red local más grande

El router de la máquina se conecta a una red local más grande (la de la planta). Una vez conectado a esta red es posible conectarse a Internet. El router de la máquina debe saber pasar de esa red más grande a Internet; normalmente la configuración necesaria para esto está disponible en un servidor DHCP instalado en la red de mayor tamaño.

Los tipos de conexión anteriores funcionan sin interrupción, por lo que es posible pasar de un extremo al otro de la red en cualquier momento.

Enrutamiento

Una parte esencial de la VPN es el enrutamiento. Para que un dispositivo en una red llegue a un dispositivo en el otro extremo no deben existir obstáculos para establecer la conexión. El dispositivo sólo necesita saber la dirección a la que debe enviar su mensaje si el destino no se encuentra dentro de la red local; es el router el encargado de gestionar la siguiente fase de la comunicación.
Cuando se recibe un mensaje, el router necesita reenviarlo a una dirección conocida. Si este router se encuentra en una red mayor, lo enviará a otro router. El mensaje se reenvía hasta que se envía por Internet o hasta que llega al dispositivo

ubicado en la red de mayor tamaño. En el caso de una conexión directa a Internet (cableada o inalámbrica), Internet se ocupará de reenviar el mensaje al destinatario.
Si el router tiene capacidad VPN y el túnel está abierto, el mensaje se reenvía a través de este túnel y llega al otro lado.

Tecnología VPN

Existen múltiples configuraciones de VPN, pero sólo dos se han mostrado seguras y fiables en la actualidad: IPSec y OpenVPN (o SSL), y ambas utilizan el mismo tipo de tecnologías de compresión y cifrado. La única diferencia es que IPsec utiliza un tipo de autenticación de nombre de usuario/contraseña, mientras que OpenVPN utiliza certificados que se deben generar en el servidor. Además, OpenVPN también utiliza el mismo método de comunicación https:// que utilizan los sitios web seguros, lo que facilita que el tráfico OpenVPN pase los firewalls de los routers, ya que este tráfico se considera seguro.

Resumen

Una red virtual privada es una conexión segura entre dos dispositivos/routers/redes. La conexión se puede establecer a través de redes locales o redes públicas, y la seguridad se establece mediante autenticación y cifrado.

Hay clientes y servidores o iniciadores y contestadores. Los clientes inician la conexión al servidor y el servidor puede aceptar conexiones de varios clientes. La conexión VPN entre el cliente y el servidor es una conexión transparente entre ambos y es posible enviar cualquier tipo de datos sin importar el extremo de la conexión VPN en que se encuentre ni la distancia entre las dos redes.

Direcciones

Dirección IP	Una dirección de protocolo de Internet (dirección IP) es una etiqueta numérica asignada a cada dispositivo (por ejemplo, un ordenador o una impresora) de una red informática que utiliza el protocolo de Internet para comunicarse.
Máscara de subred	Una máscara de subred es una subdivisión lógicamente visible de una dirección IP en una dirección de red y una dirección de nodo. Cuando una red se divide en dos o más redes, se denominan subredes. Si una dirección IP no se encuentra dentro de la red local, el mensaje se enviará al router o a la puerta de enlace.
DHCP	El protocolo de configuración dinámica de host es un protocolo de red que se emplea para configurar los dispositivos que están conectados a una red para que se puedan comunicar en esa red utilizando el protocolo de Internet (IP). El protocolo se implementa en un modelo cliente-servidor, en el que los clientes DHCP solicitan los datos de configuración, como una dirección IP, una ruta por defecto, y una o más direcciones de servidor DNS del servidor DHCP.
Dirección de red local y remota	La dirección de red local se determina al combinar la dirección IP con la máscara de subred y se ejecuta la operación lógica AND. Con la dirección IP 192.168.250.12 y una máscara de subred 255.255.255.0, la dirección de red local es 192.168.250.0 y tiene un intervalo de 1 a 254. Si la dirección IP no está dentro de este rango se trata de una dirección remota. En VPN también podría ser una dirección de red remota.
Dirección de puerta de enlace	La dirección de puerta de enlace (o puerta de enlace predeterminada) es una interfaz de router conectada a la red local que envía paquetes fuera de la red local.
Dirección de servidor DNS	El sistema de nombres de dominio (DNS) traduce fácilmente los nombres de dominio memorizados en direcciones IP numéricas convirtiendo los nombres en direcciones. El servidor DNS tiene una dirección IP fija para sí. Por ejemplo, el nombre www.omron.com se traduce a 202.232.86.142

Componentes

Router/puerta de enlace	Un router es un dispositivo que envía paquetes de datos entre redes de ordenadores, y puede tratarse de dos redes o de una red local e Internet. Si el router reenvía un paquete a una red más grande también se denomina puerta de enlace.
Servidores DHCP, DNS y NTP	Un servidor es accesible localmente o en Internet y ofrece un servicio. Un servidor DHCP asigna direcciones IP. Un servidor DNS traduce nombres a direcciones IP. Un servidor NTP asigna una hora a un dispositivo.
Iniciador y contestador VPN	Una conexión VPN se inicia siempre desde un extremo. Por lo tanto, uno de los extremos espera a responder la solicitud del iniciador. Es comparable al principio de funcionamiento cliente/servidor.
UMTS, ADSL, cable y fibra	Diferentes tecnologías para conectarse a Internet mediante una conexión inalámbrica, cableada o de fibra óptica.
LAN y WAN	Red de área local frente a red de área amplia. En una red LAN todos los dispositivos están en la misma ubicación, como una oficina o una planta. La red WAN es más grande que la red LAN y está conectada a través de un router.

Servicios

VLAN	La red de área local virtual es una tecnología en la que se combinan varios puertos de un switch gestionado en una especie de "red física". El tráfico del resto de puertos de ese switch (o de otros) no aparece en los puertos asignados a la VLAN. Una VLAN puede abarcar varios switches de una red LAN. La razón de ser de estas redes es separar el tráfico.
Enrutamiento	Es el proceso de selección de trayectorias de una red por las que se envía el tráfico de la red.
Firewall	Un firewall es un sistema de seguridad basado en software o en hardware que controla el tráfico entrante y saliente analizando los paquetes de datos y determinando si se dejan pasar o no, según un conjunto de reglas. Un firewall establece una barrera entre una red interna segura y fiable, y otra red (p. ej., Internet) que no se considera segura ni fiable.
Protocolo VPN	VPN (red virtual privada) es un término general. Existen muchos protocolos/implementaciones diferentes y unos son más seguros que otros. Las implementaciones más utilizadas actualmente son IPSec y OpenVPN.

Omron Corporation

- 50 años en automatización industrial
- Más de 35.000 empleados
- Asistencia en todos los países de Europa
- Más de 1.800 empleados en 19 países de Europa
- 800 ingenieros especializados
- 7% de la facturación invertido en I+D
- Más de 200.000 productos
- Más de 6.950 patentes registradas hasta la fecha

Omron Industrial Automation

Con sede en Kioto, Japón, OMRON Corporation es un líder a nivel mundial en el sector de la automatización. Fundada en 1933 y con su presidente Hisao Sakuta, a la cabeza, Omron cuenta con más de 35.000 empleados en más de 35 países dedicados a proporcionar productos y servicios a clientes de una amplia variedad de campos, entre otros, la automatización industrial, componentes electrónicos y de salud. La compañía está dividida en cinco regiones con oficinas centrales en Japón (Kioto), Asia Pacífico (Singapur), China (Hong Kong), Europa (Ámsterdam) y Estados Unidos (Chicago). La región europea cuenta con sus propias instalaciones de fabricación y desarrollo, así como con un servicio de atención al cliente propio para todos los países europeos.

Si desea obtener más información, visite el sitio web de Omron en www.industrial.omron.eu

AUTOR

René Heijma
Product Specialist Industrial Communication

- Omron Europe B.V.
  Product Marketing Automation department
- Zilverenberg 2,
  5234GM, 's-Hertogenbosch,
  Países Bajos
- Tel. +31 (0)73 6481 950
- rene.heijma@eu.omron.com
- industrial.omron.eu/packaging

René Heijma comenzó su carrera profesional como ingeniero de PLC y SCADA y participó en multitud de proyectos de automatización de máquinas y procesos, desde las fases iniciales de especificaciones, la programación de sistemas PLC y SCADA, y hasta la puesta en servicio de las instalaciones.

Llegó a Omron en 2001 como especialista de redes. Por entonces DeviceNet y PROFIBUS eran las redes que necesitaban un mayor nivel de especialización, pero desde que las redes basadas en Ethernet resurgieron, René se especializó en estas tecnologías. También se ha especializado en nuevos productos y en su integración en Omron.

La tecnología VPN no pertenece en realidad al dominio de redes de control, si bien se considera una extensión de gran atractivo. René ha investigado cómo aplicar estas tecnologías a las aplicaciones de Omron. Este documento técnico es un resumen de esta investigación.