Seguridad para los servicios empresariales PON

Boletín

Para tener éxito en la oferta de servicios empresariales, la seguridad es primordial. Como medio compartido, PON utiliza varios métodos para separar, cifrar y proteger los datos en la red, con el fin de ofrecer una seguridad de misión crítica equiparable a la de las conexiones dedicadas punto a punto. En este artículo se explican los distintos métodos.

Autores: Yannick Sillis, Aravindan Jagannathan

Índice

Introducción

La disponibilidad comercial de las tecnologías PON 10G y PON 25G de alta capacidad presenta a los operadores de redes de banda ancha de fibra nuevas oportunidades en servicios mayoristas, de convergencia y, sobre todo, comerciales.

Una única infraestructura PON de alta capacidad puede soportar cómodamente los requisitos de servicios empresariales con SLA garantizados, junto con backhaul móvil y servicios residenciales premium. Esto permite a los operadores reducir significativamente los costes y crear una ventaja competitiva a través de precios más atractivos.

Consideraciones de seguridad

Para tener éxito en la oferta de servicios empresariales, es fundamental proporcionar una conectividad segura.

PON tiene una arquitectura punto a multipunto, en la que una fibra se divide para dar servicio a varios usuarios. Pero si varios usuarios comparten una fibra, ¿hasta qué punto son seguras las redes punto a multipunto? Las normas PON se han esforzado mucho por definir las características que garanticen la seguridad de los datos transferidos a través de una PON. Esto permite a los operadores beneficiarse de una solución más rentable para conectar a todo el mundo, al tiempo que ofrecen seguridad de misión crítica a sus clientes.

Analicemos los posibles problemas de seguridad y cómo los resuelve la tecnología PON.

En el sentido ascendente (del usuario a la red), el módem de un usuario (llamado ONU) envía tráfico en una sola dirección: al nodo de acceso de fibra (llamado OLT). La señal no se refleja en la red, por ejemplo, desde los divisores o las OLT, porque estos dispositivos están diseñados y fabricados para no reflejar prácticamente nada. Por tanto, no es posible que el tráfico enviado por un ONU sea interceptado por otro ONU.

En sentido descendente, es decir, de la red al usuario, la OLT envía tráfico a todas las ONU. Pero esto no significa que las ONU puedan leer los datos destinados a otros usuarios. En una PON, cada paquete está etiquetado y una ONU sólo puede recibir los paquetes que le están destinados.

Para interferir en el tráfico de una PON (ya sea para interceptarlo o transmitirlo), un usuario malintencionado tendría que insertar una ONU (u otro dispositivo de escucha) antes o después del divisor, o sustituir el propio divisor por otro muy reflectante que reflejara el tráfico hacia la ONU malintencionada o legítima.

Todo esto es extremadamente difícil de hacer sin ser detectado debido a la naturaleza física de una red de fibra óptica. Cualquier dispositivo introducido en la red necesita una conexión física, lo que interrumpirá las señales en la red y debería activar una alarma. Además, aunque fuera posible fabricar un divisor altamente reflectante, sus ubicaciones (normalmente bajo tierra o en lugares de difícil acceso) no son de dominio público.

Sin embargo, “extremadamente difícil” no es lo mismo que “imposible”, por lo que las redes PON utilizan diversos métodos para separar, cifrar y proteger los datos en la red, con el fin de proporcionar una seguridad de extremo a extremo y de misión crítica equiparable a la de las conexiones dedicadas punto a punto (que, por supuesto, son igual de susceptibles a los dispositivos de escucha insertados maliciosamente).

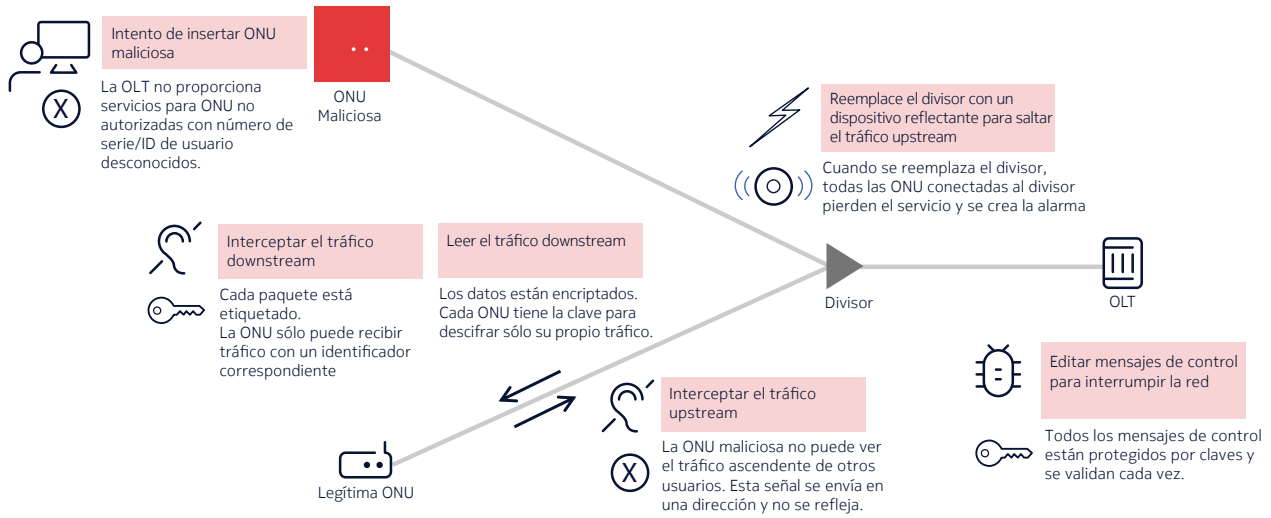
Funciones de seguridad PON

Las redes PON utilizan varias funciones de seguridad para:

- Aislar el tráfico para cada usuario
- Cifrar el tráfico de datos
- Impedir la conexión de dispositivos no autorizados
- Validar los mensajes de control

Estas características de seguridad dependen de la estructura de paquetes utilizada en la transmisión de datos PON. Cada paquete de datos está compuesto por la carga útil (la información de usuario que se transmite) y una cabecera que incluye información sobre la transmisión (como su longitud, origen y destino) e información de seguridad (claves de cifrado, códigos de intervalo de tiempo, etc.).

Figura 1. Las funciones de seguridad de PON garantizan la protección de los datos de misión crítica



Aislamiento del usuario

Cada ONU recibe todos los datos downstream de la OLT. Esto aumenta la posibilidad de que alguien intente leer el tráfico downstream destinado a otro usuario.

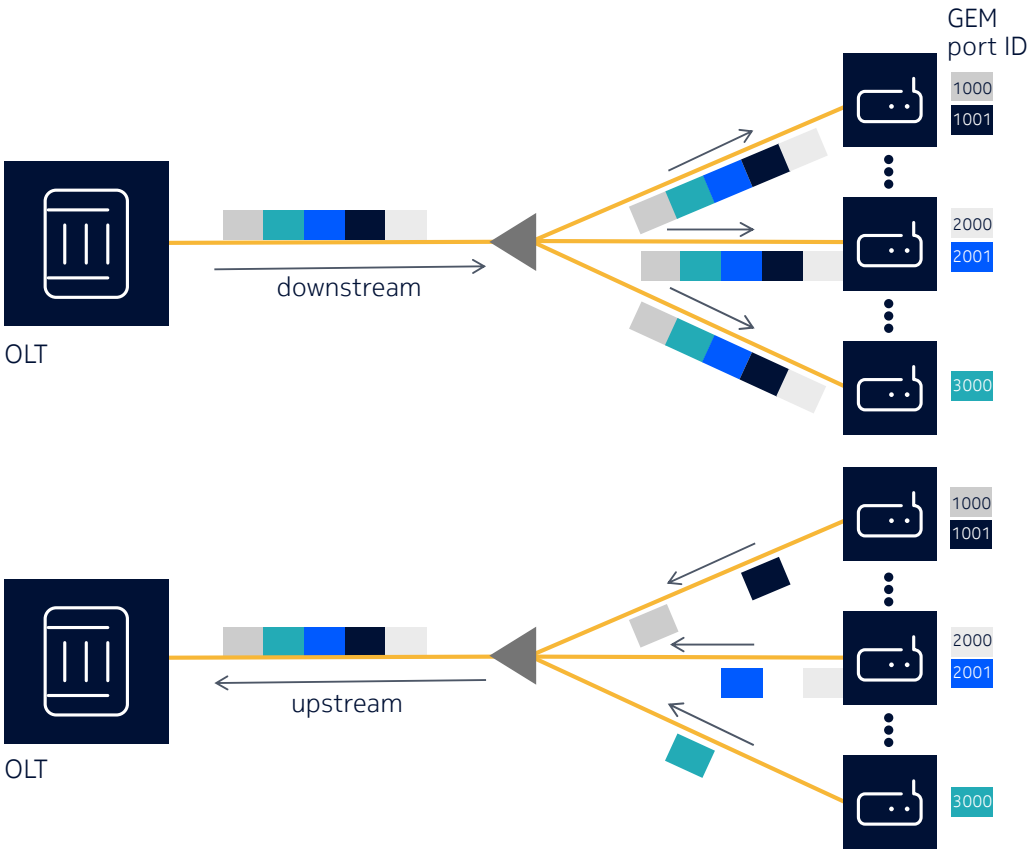
La tecnología PON utiliza Gigabit Encapsulation Method (GEM), que es una etiqueta en la cabecera, para aislar el tráfico de cada usuario. Para el tráfico downstream, el GEM indica a las ONU qué paquete es para ellas y, para el tráfico de subida, indica a la OLT de qué usuario o servicio procede ese paquete.

En la transmisión downstream, aunque un ONU recibe paquetes de datos para todos los abonados, sólo puede recibir estos paquetes con un identificador correspondiente en el GEM. Un ONU malintencionado en la red no habrá sido provisto de un identificador GEM reconocido y, por tanto, no podrá recibir ningún paquete.

En la transmisión upstream, cada ONU transmite directamente a la OLT a intervalos de tiempo asignados. Los datos upstream no se reflejan en la OLT ni en el divisor óptico pasivo, por lo que otros ONU no pueden oír el tráfico upstream. Si un ONU malintencionado se introduce de algún modo en la red sin activar una

alarma, seguirá sin ser reconocido en la base de datos de aprovisionamiento del OLT y no se le asignarán intervalos de tiempo para enviar sus datos.

Figura 2: Aislamiento de usuarios en una PON



Codificación del tráfico

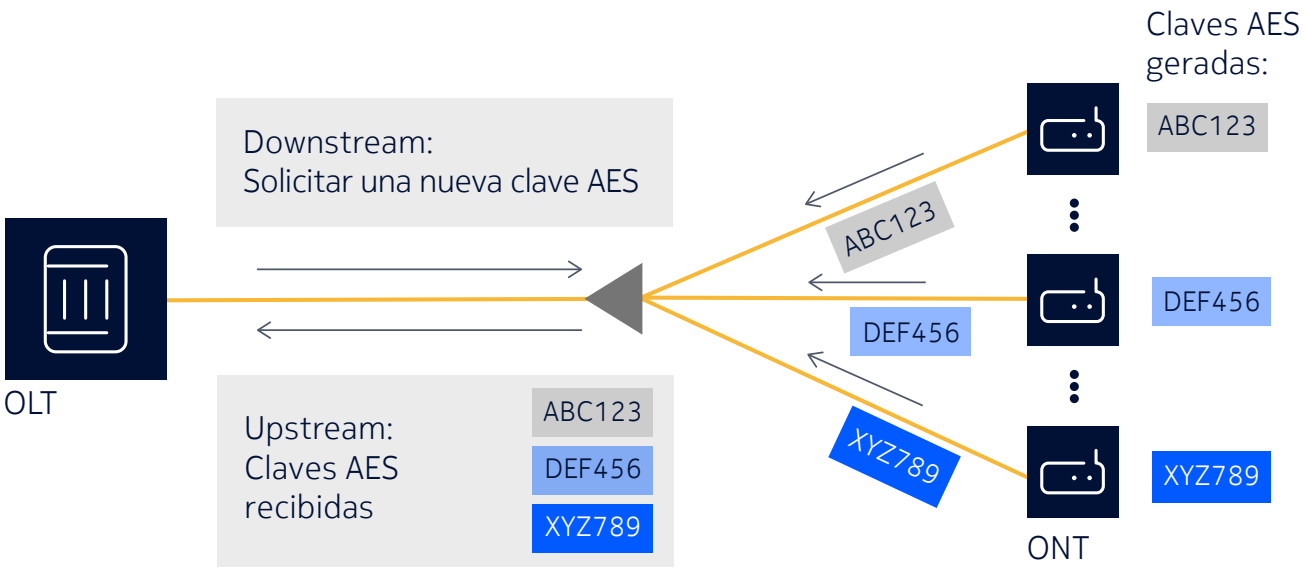
Además de separar los datos de cada usuario, los propios datos se protegen mediante cifrado.

Las redes PON utilizan el conocido algoritmo de seguridad Advanced Encryption Standard (AES) para cifrar los paquetes de datos. Todos los paquetes que entran o salen de una ONU se cifran con la clave, que sólo conocen esa ONU y la OLT.

Las claves de cifrado son generadas por cada ONU y enviadas en sentido upstream a la OLT. Se actualizan periódicamente (por ejemplo, cada hora o cada día), dependiendo de la configuración de la red. Como ya se ha mencionado, el tráfico no se refleja en la red, por lo que otros ONU no pueden interceptar las claves (además, las claves de cifrado se cifran cuando se envían).

El cifrado se aplica tanto a la carga útil de datos como a la de GEM, lo que proporciona un nivel adicional de seguridad para que las tramas GEM no puedan leerse, aunque sean interceptadas.

Figura 3. El cifrado AES impide el espionaje



Activación del usuario

El PON dispone de un procedimiento de activación del usuario que impide la conexión de dispositivos no autorizados. Cada ONU tiene un número de serie y un ID de registro únicos. El número de serie se establece en fábrica y se codifica en el hardware del ONU; el ID de registro de cada nuevo abonado lo asigna el operador y se establece en el ONU cuando se instala.

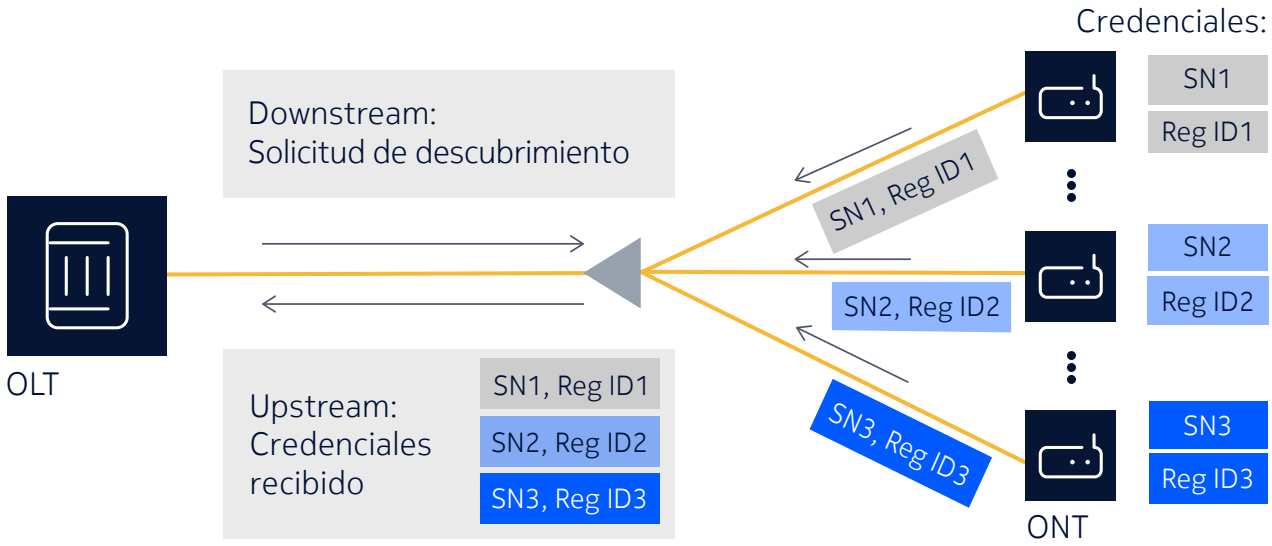
El operador también programa el número de serie y el ID de registro en los datos de aprovisionamiento, de modo que la OLT conoce de antemano todas las ONU que deben recibir el servicio.

Cuando se introduce un ONU en la red, el proceso de aprovisionamiento comprueba la autenticidad de estos códigos: la OLT solicita los códigos al ONU y comprueba que coinciden con lo esperado. Los códigos se entregan upstream, por lo que no pueden ser interceptados por otro ONU.

Una ONU introducida maliciosamente no tendrá una combinación correcta de número de serie e ID de registro, por lo que la OLT no le proporcionará ningún servicio.

Como ocurre con cualquier mecanismo de seguridad, el ser humano es el eslabón más débil. Es posible que alguien pueda obtener el número de serie y el identificador de registro de una ONU legítima en la red. Sin embargo, esto es tan difícil como obtener la contraseña de alguien u otra información sensible, porque requiere acceso físico a la ONU legítima para leer el número de serie, iniciar sesión en la interfaz local de la ONU u obtener la carta o el correo para recuperar el ID de registro.

Figura 4: La activación del usuario impide que ONU no autorizadas accedan a la PON



Integridad de los mensajes

En una PON, una ONU es activada, configurada, gestionada y supervisada por la OLT. Un usuario malintencionado puede intentar generar, replicar o editar mensajes de control que podrían provocar una interrupción del servicio. Por ejemplo, un usuario malintencionado podría intentar generar alarmas de red (por ejemplo, una alarma de pérdida de LAN) que desencadenaran una interrupción del servicio.

Las comprobaciones de integridad de los mensajes (MIC: Message Integrity Checks) son utilizadas por la OLT y las ONU para verificar que los mensajes de control downstream y upstream proceden de una fuente legítima y no han sido manipulados. En sentido Downstream, la OLT genera e inserta un MIC cuando se transmite un mensaje y la ONU lo verifica cuando lo recibe. En Upstream, la ONU genera e inserta un MIC cuando se transmite el mensaje y la OLT lo verifica cuando lo recibe.

Para cada ONU hay un conjunto específico de claves que se utilizan para generar el MIC. Estas claves MIC son calculadas por la OLT y la ONU de forma independiente, basándose en la información intercambiada bidireccionalmente durante el proceso de activación de la ONU, como el número de serie y el ID de registro de la ONU. Por lo tanto, sólo la OLT y la ONU tienen toda la información necesaria para generar y validar la MIC para los mensajes de control relacionados con esa ONU.

Los MIC se ejecutan en la capa de control y protegen contra un usuario malintencionado que intente interrumpir una red en lugar de robar datos de ella.

Conclusión

Las cuatro funciones de seguridad que se explican en este artículo se combinan para proporcionar seguridad de misión crítica en redes PON. El tráfico de usuario está protegido por encriptación AES. Los mensajes de control se transmiten en código GEM, por lo que también están cifrados. Además, se comprueba la integridad de los mensajes. Combinados, proporcionan la máxima protección contra la interceptación de datos, así como la máxima protección de los propios datos.

El nivel de seguridad de una PON es equivalente al de cualquier acuerdo de nivel de servicio para un servicio de banda ancha punto a punto. Esto allana el camino para que los operadores adopten con confianza la PON para prestar servicios empresariales y aprovechen la PON 10G y la PON 25G para converger servicios, reducir costes y generar nuevos ingresos.

Abreviaturas

AES	Cifrado estándar avanzado
GEM	Método de encapsulación Gigabit
MIC	Comprobación de la integridad de los mensajes
OLT	Terminal de línea óptica
ONU	Unidad de red óptica
PON	Red óptica pasiva
SLA	Acuerdo de nivel de servicio

Nokia OYJ

Karakaari 7

02610 Espoo

Finlandia

Tel. +358 (0) 10 44 88 000

CID 214574