Segurança para PON Business Services

Informativo

Para ter sucesso na oferta de serviços empresariais, a segurança é fundamental. Como um meio compartilhado, a PON usa vários métodos para separar, criptografar e proteger dados na rede para fornecer segurança de missão crítica em pé de igualdade com conexões ponto a ponto dedicadas. Este artigo explica os vários métodos envolvidos.

Autores: Yannick Sillis, Aravindan Jagannathan

Índice

Introdução

A disponibilidade comercial das tecnologias PON 10G e PON 25G de alta capacidade apresenta às operadoras de redes de banda larga de fibra novas oportunidades no atacado, na convergência e, principalmente, nos serviços comerciais.

Uma única infraestrutura da PON de alta capacidade pode suportar confortavelmente os requisitos para serviços empresariais com SLAs garantidos, junto com backhaul móvel e serviços residenciais de nível premium. Isso permite que as operadoras reduzam significativamente os custos e criem uma vantagem competitiva por meio de preços mais atraentes.

Considerações de segurança

Para ter sucesso na oferta de serviços empresariais, fornecer conectividade segura é fundamental.

A PON tem uma arquitetura ponto-a-multiponto, onde uma fibra é dividida para atender a vários usuários. Mas se vários usuários compartilham uma fibra, quão seguras são as redes ponto a multiponto? Os padrões da PON se esforçaram muito para definir os recursos que garantirão a segurança dos dados transferidos por meio de uma PON. Isso permite que as operadoras se beneficiem de uma solução mais econômica para conectar todos e, ao mesmo tempo, oferecer segurança de missão crítica para seus clientes.

Vamos explorar possíveis preocupações de segurança e como a tecnologia da PON as resolve.

Na direção upstream (do usuário para a rede), o modem de um usuário (chamado ONU) envia o tráfego apenas em uma direção - para o nó de acesso de fibra (chamado OLT). O sinal não é refletido de volta para a rede, por exemplo, de divisores ou OLTs, porque esses dispositivos são projetados e fabricados para refletir quase nenhuma luz. Portanto, não é possível que o tráfego enviado por uma ONU seja interceptado por outra ONU.

Na direção downstream, que é da rede para o usuário, o OLT envia tráfego para todas as ONUs. Mas isso não significa que as ONUs possam ler os dados destinados a outros usuários. Em uma PON, cada pacote é rotulado e uma ONU pode receber apenas os pacotes destinados a ele.

Para interferir no tráfego em uma PON (seja para interceptar ou transmitir), um usuário mal-intencionado precisaria inserir uma ONU (ou outro dispositivo de escuta) antes ou depois do divisor, ou substituir o próprio divisor por um altamente reflexivo que refletiria de volta para a ONU maliciosa ou legítima.

Tudo isso é extremamente difícil de fazer sem ser detectado devido à natureza física de uma rede de fibra óptica. Qualquer dispositivo introduzido na rede precisa de uma conexão física, o que interromperá os sinais na rede e deverá acionar um alarme. Além disso, mesmo que fosse possível fabricar um divisor altamente reflexivo, suas localizações (tipicamente subterrâneas ou em locais de difícil acesso) não são conhecidas publicamente.

No entanto, “extremamente difícil” não é o mesmo que “impossível”, portanto, as redes PON usam vários métodos para separar, criptografar e proteger dados na rede para fornecer segurança de ponta a ponta e de missão crítica em pé de igualdade com conexões ponto a ponto dedicadas (que, é claro, têm a mesma suscetibilidade a dispositivos de escuta inseridos maliciosamente).

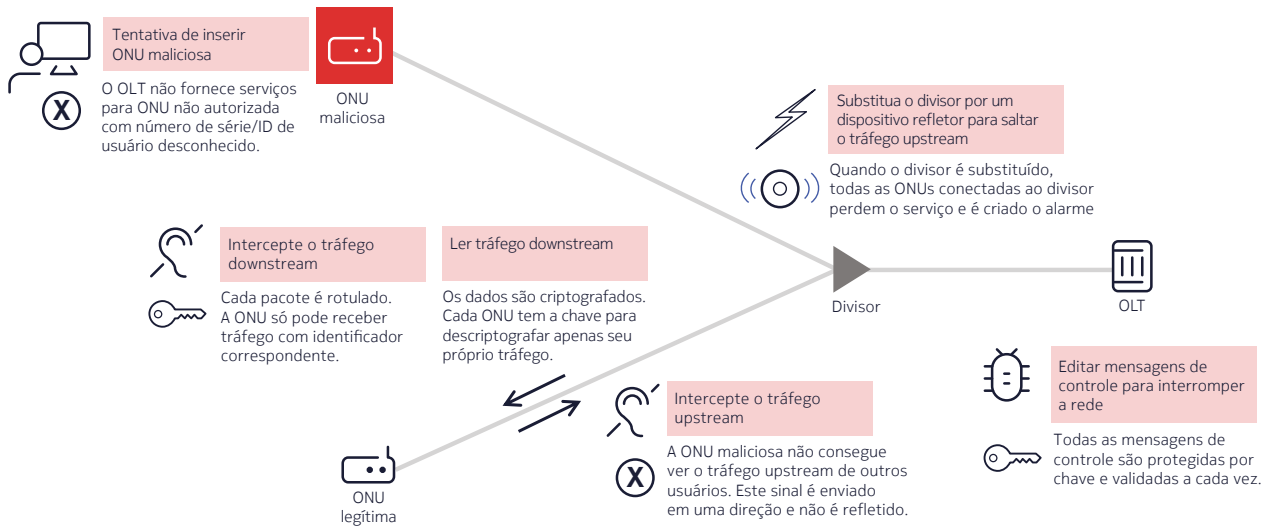
Recursos de segurança da PON

As redes de PON usam vários recursos de segurança para:

- Isolar o tráfego para cada usuário
- Criptografar o tráfego de dados
- Impedir que dispositivos não autorizados sejam conectados
- Validar mensagens de controle

Esses recursos de segurança dependem da estrutura de pacotes usada na transmissão de dados PON. Cada pacote de dados é composto pela carga útil (as informações do usuário sendo transmitidas) e um cabeçalho compreendendo informações sobre a transmissão (como seu comprimento, origem e destino) e informações de segurança (chaves de criptografia, códigos de intervalo de tempo, etc.).

Figura 1. Os recursos de segurança da PON garantem a proteção de dados de missão crítica



Isolamento do usuário

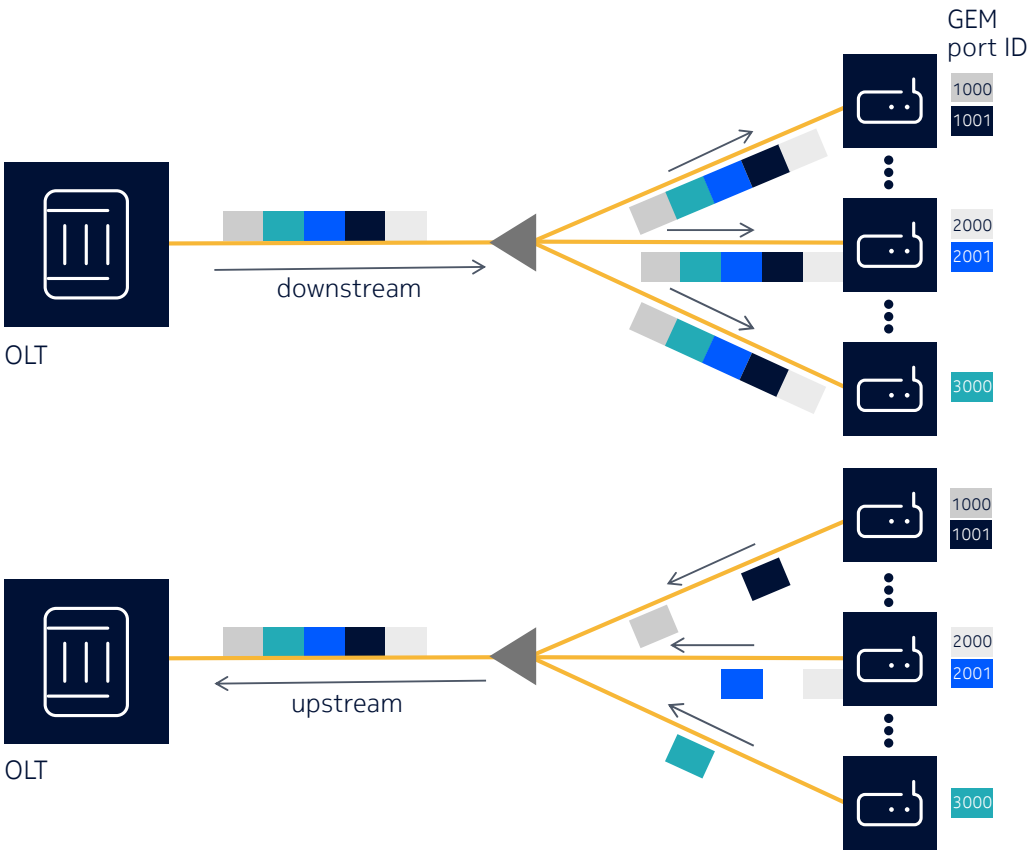
Toda ONU recebe todos os dados downstream do OLT. Isso aumenta o potencial de alguém tentar ler o tráfego downstream destinado a outro usuário.

A tecnologia PON usa o Gigabit Encapsulation Method (GEM), que é um rótulo no cabeçalho, para isolar o tráfego para cada usuário. Para o tráfego downstream, o GEM informa à ONUs qual pacote é para ele e, para o tráfego de upload, informa ao OLT de qual usuário ou serviço esse pacote se origina.

Na transmissão downstream, embora uma ONU receba pacotes de dados para todos os assinantes, ela só pode receber esses pacotes em um identificador correspondente na GEM. Uma ONU maliciosa na rede não terá sido provisionada com um identificador GEM reconhecido e, portanto, não poderá receber nenhum pacote.

Na transmissão a upstream, cada ONU transmite diretamente para o OLT em intervalos de tempo atribuídos. Os dados upstream não são refletidos de volta do OLT ou do divisor óptico passivo, de modo que outras ONUs não podem ouvir o tráfego upstream. Se uma ONU maliciosa for de alguma forma inserida na rede sem disparar um alarme, ela ainda não será reconhecida no banco de dados de provisionamento do OLT e não receberá intervalos de tempo para enviar seus dados.

Figura 2. Isolamento de usuário em uma PON



Criptografia de tráfego

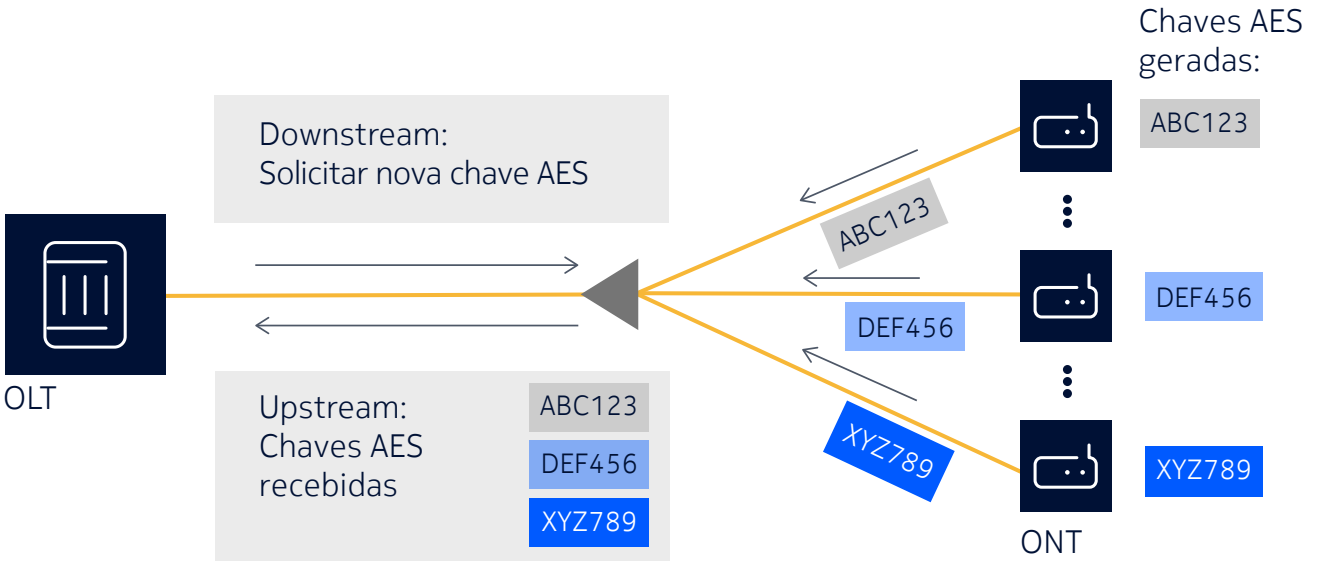
Além de separar os dados de cada usuário, os dados em si são protegidos por criptografia.

As redes PON usam o conhecido algoritmo de segurança Advanced Encryption Standard (AES) para criptografar pacotes de dados. Todos os pacotes provenientes de ou para uma ONU são criptografados com a chave, que só é conhecida por essa ONU e pelo OLT.

As chaves de criptografia são geradas por cada ONU e enviadas upstream para o OLT. Eles são atualizados periodicamente (por exemplo, de hora em hora, diariamente), dependendo da configuração da rede. Como mencionado anteriormente, o tráfego não é espelhado de volta na rede, portanto, outras ONUs não podem interceptar as chaves (também as chaves de criptografia são criptografadas quando enviadas).

A criptografia é aplicada tanto à carga útil de dados quanto à carga útil do GEM, fornecendo um nível adicional de segurança, de modo que os quadros do GEM não podem ser lidos mesmo se interceptados.

Figura 3. A Criptografia AES evita espionagem



Ativação do usuário

A PON possui um procedimento de ativação do usuário que impede que dispositivos não autorizados sejam conectados. Cada ONU tem um número de série e ID de registro exclusivos. O número de série é definido na fábrica e é codificado no hardware da ONU; o ID de registro para cada novo assinante é atribuído pelo operador e definido na ONU quando é instalado.

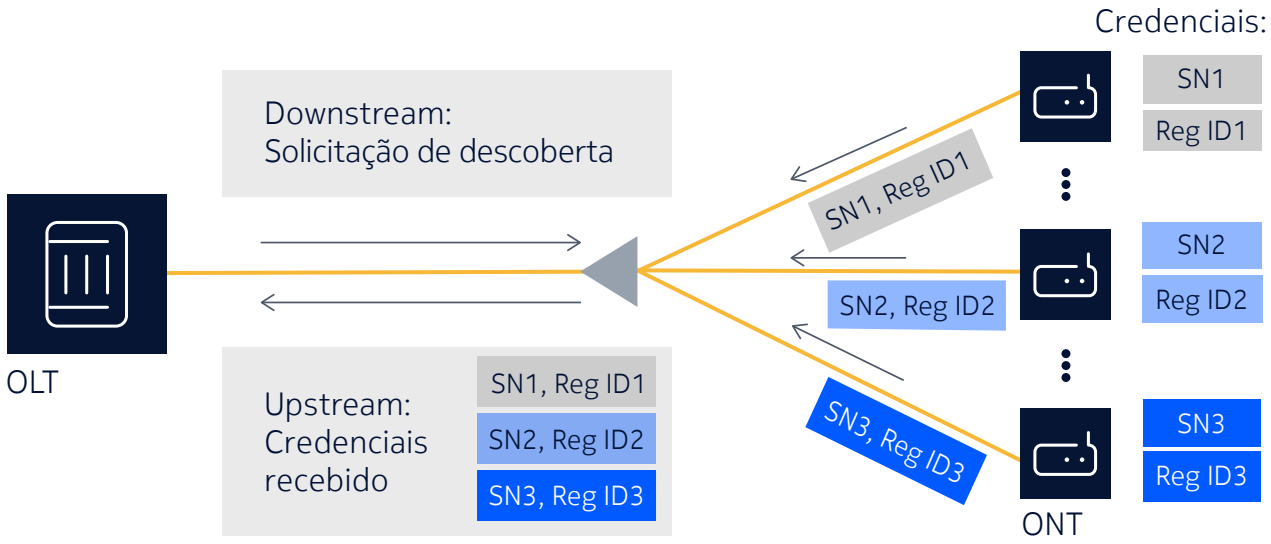
O número de série e o ID de registro também são programados pelo operador nos dados de provisionamento, para que o OLT saiba antecipadamente todas as ONUs que devem receber o serviço.

Quando uma ONU é introduzida na rede, o processo de provisionamento verifica a autenticidade desses códigos: o OLT solicita os códigos da ONU e verifica se eles correspondem ao esperado. Os códigos são entregues upstream, portanto não podem ser interceptados por outra ONU.

Uma ONU introduzida maliciosamente não terá uma combinação correta de número de série e ID de registro; portanto, o OLT não fornecerá nenhum serviço a ela.

Como em qualquer mecanismo de segurança, os humanos são o elo mais fraco. É possível que alguém possa obter o número de série e o ID de registro de uma ONU legítima na rede. No entanto, isso é tão difícil quanto obter a senha de alguém ou outras informações confidenciais, porque requer acesso físico à ONU legítima para ler o número de série, fazer login na interface local da ONU ou obter a carta ou correio para recuperar o ID de registro.

Figura 4. A ativação do usuário impede que ONUs não autorizadas acessem a PON



Integridade da mensagem

Em uma PON, uma ONU é ativada, configurada, gerenciada e monitorada pelo OLT. Um usuário mal-intencionado pode tentar gerar, replicar ou editar mensagens de controle que possam causar interrupção do serviço. Por exemplo, um usuário mal-intencionado pode tentar gerar alarmes de rede (por exemplo, um alarme de perda de LAN) que desencadearia uma interrupção do serviço.

As verificações de integridade de mensagens (MIC) são usadas pelo OLT e ONUs para verificar se as mensagens de controle downstream e upstream vêm de uma fonte legítima e se não foram adulteradas. Downstream, é gerado um MIC e inserido pelo OLT quando uma mensagem é transmitida e verificada pela ONU quando recebida. Upstream, é gerado um MIC e inserido pela ONU quando a mensagem é transmitida e verificada pelo OLT quando recebido.

Para cada ONU, há um conjunto dedicado de chaves usadas para gerar o MIC. Essas chaves MIC são calculadas pelo OLT e pela ONU de forma independente, com base em informações trocadas bidirecionalmente durante o processo de ativação da ONU, como o número de série da ONU e o ID de registro. Portanto, apenas o OLT e a ONU têm todas as informações necessárias para gerar e validar o MIC para mensagens de controle relacionadas a essa ONU.

Os MICs são executados na camada de controle e são uma proteção contra um usuário mal-intencionado que tenta interromper uma rede, em vez de roubar dados dela.

Conclusão

Os quatro recursos de segurança explicados neste artigo se combinam para fornecer segurança de missão crítica em redes PON. O tráfego do usuário é protegido por criptografia AES. As mensagens de controle são transportadas no código GEM, portanto, também são criptografadas. Além disso, há verificações de integridade de mensagens. Combinados, eles fornecem a máxima proteção contra a interceptação de dados, bem como a máxima proteção dos próprios dados.

O nível de segurança em uma PON é o equivalente ao nível de segurança fornecido em qualquer SLA para um serviço de banda larga ponto a ponto. Isso abre caminho para que as operadoras adotem com confiança a PON para fornecer serviços comerciais e aproveitar a PON 10G e a PON 25G para convergir serviços, reduzir custos e gerar novas receitas.

Abreviações

AES	Criptografia Padrão Avançada
GEM	Método de Encapsulamento Gigabit
MIC	Verificação da integridade da mensagem
OLT	Terminal de linha óptica
ONU	Unidade de rede óptica
PON	Rede óptica passiva
SLA	Acordo de nível de serviço

CID: 213790