

Trabalho de Redes II - Protocolo IEEE 802.1X

Carlos Valente, Gustavo Constante, Maciel Vinícius, Anderson Demétrio

16/03/2016

Índice:

- Introdução
- O que é e para que foi projetado
- Estrutura do protocolo
- Método de comunicação
- Aplicações
- Referências:

Introdução:

Este trabalho tem como principal objetivo mostrar o funcionamento do protocolo 802.1X, discutir o motivo e a necessidade que fizeram com que ele fosse projetado, suas implementações e exemplificar o seu funcionamento.

Trataremos primeiro de explicar o que é o protocolo e para que ele foi projetado, depois mostraremos a estrutura do protocolo, descrevendo brevemente os campos de seu cabeçalho.

Será apresentado um fluxograma de comunicação do protocolo para que o método de comunicação seja explicado de uma maneira mais simples para o entendimento do público geral.

Por fim listaremos algumas aplicações e locais onde o protocolo é aplicado com frequência e explicaremos o porquê de ele ser usado na devida aplicação.

O que é e para que foi projetado.

O standard 802.1x é uma solução de segurança, criada pelo IEEE, permitindo autenticar um utilizador que deseja ter acesso a uma rede (com fios ou não) graças a um servidor de autenticação baseado em portas (PNAC). Tem como base o protocolo EAP, que tem como função transportar as informações de identificação dos utilizadores.

A autenticação ainda disponibiliza um bloqueio adicional para intranet, usada para que máquinas convidadas, convidados e dispositivos não gerenciados que não executam uma autenticação bem-sucedida conectem-se a intranet da sua empresa. Normalmente o 802.1x é usado como um meio de segurança avançado para redes com fio. Porém estão agora procurando usar para segurança de redes sem fio. Isso porque um cliente wireless precisa executar autenticação antes de enviar dados.

O padrão IEEE 802.1X, é simplesmente um padrão para a passagem de EAP através de uma LAN com fio ou sem fio. Com o 802.1X você empacota mensagens EAP em quadros Ethernet e não usa PPP. É a autenticação e nada mais. Os gestores de TI buscam isso em situações nas quais o PPP não é necessário, quando eles usam protocolos diferentes de TCP/IP ou quando a sobrecarga e a complexidade de usar PPP é indesejável.

Estrutura do protocolo.

São utilizados dois protocolos bases para implementar o padrão IEEE 802.1x que são o EAP e RADIUS. Estes protocolos são necessários para cada etapa de interação entre os equipamentos.

Quando se conecta o cabo ao Switch que possui o protocolo 802.1X ativo, a porta inicialmente entra em modo “não autorizado”, onde são permitidos apenas pacotes 802.1X e os demais são descartados.

EAPoL - Extensible Authentication Protocol over Lan, este protocolo é utilizado para realizar as trocas de informações para autenticação entre o requerente (cliente) e o autenticador (switch). Ele se baseia no protocolo EAP e seu quadro é formado seis campos.

Cabeçalho MAC	Tipo Ethernet	Versão	Tipo de pacote	Comprimento	Corpo	Checksum
12 bytes	2 bytes	1 byte	1 byte	2 bytes	variável	4 bytes

Cabeçalho MAC - É formado pelo endereço MAC de origem e destino.

Tipo Ethernet - É o código que foi atribuído ao protocolo EAPoL.

Versão - Em 2004 foi padronizada a última versão que não se modificou.

Tipo de Pacote - Representa o tipo de quadro que será enviado, EAPoL-Start, EAPoL-Logoff, EAP-Packet, EAPoL-Key.

Comprimento - É um campo que define o comprimento do quadro.

Corpo - Informação que será utilizada na negociação.

Checksum - soma do quadro para verificação de erro.

RADIUS - Remote Authentication Dial In User Service, este protocolo tem a função de realizar a comunicação entre o Switch que recebeu uma solicitação de autenticação e a confirmação da identidade com o servidor que armazena estes parâmetros. O protocolo RADIUS possui cinco campos que compõem seu quadro.

Código	Identificador	Comprimento	Autenticador	Atributos
1 byte	1 byte	2 bytes	16 bytes	variável

Código - Identifica o tipo de pacote RADIUS que esta sendo enviado/recebido.

Identificador - Utilizado para identificar as requisições e respostas

Comprimento - É o tamanho total do quadro RADIUS, neste campo está incluso o tamanho de todos os demais campos incluindo o próprio comprimento.

Autenticador - Neste campo estão armazenados os valores utilizados para autenticar as repostas e também algum outro algoritmo de ocultação.

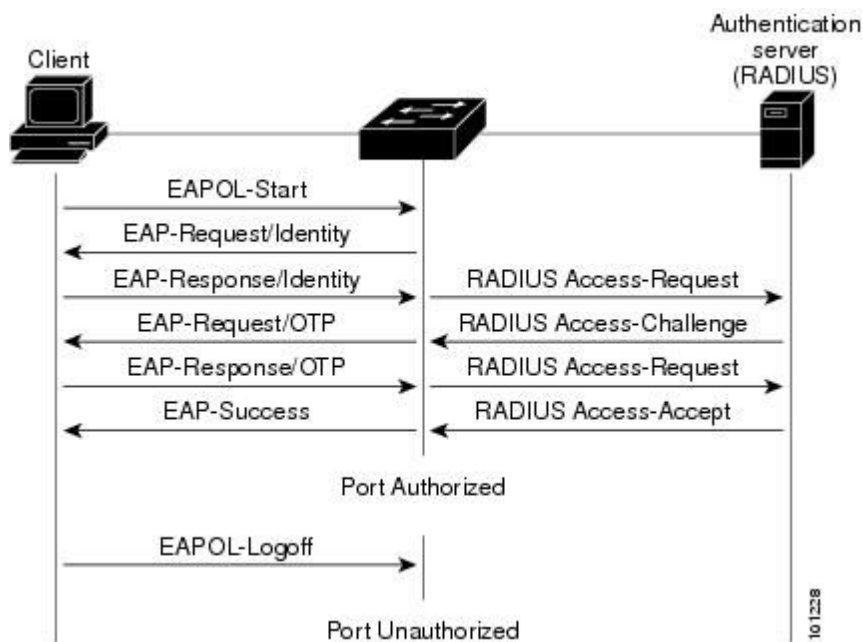
Atributos - Carrega informações de autenticação ou autorização, e alguns detalhes específicos de uma requisição ou determinada resposta.

Método de comunicação

No 802.1X temos os conceitos de entidades, que no caso são três:

- Suplicante, corresponde ao software no pc que é responsável por solicitar a autenticação e fazer a comunicação com o switch.
- Autenticador, é o switch que intermediária a autenticação.
- Servidor, é a máquina servidor responsável por realizar a autenticação das solicitações.

O fluxo de solicitações ocorre da seguinte maneira:



Após todas as etapas o switch libera ou não a porta para o fluxo de pacotes ethernet.

Aplicações

Access Point - Vendedores de *access points Wi-Fi* agora usam 802.1X para *access points wireless* com o intuito de corrigir as vulnerabilidades de segurança encontradas em WEP. O papel do autenticador é realizado tanto pelo *Access point* em si via chave-pré-compartilhada ou para empresas maiores, por identidade terceira, como um servidor RADIUS. Ele provê autenticação apenas para o cliente ou, mais apropriadamente, autenticação forte e mútua utilizando protocolos como EAP-TLS.

Software - Alguns sistemas operacionais tem implementado por default o 802.1X. Os sistemas operacionais windows mais recentes são um exemplo disso, Existem versões mais antigas que possuem também o 802.1X, mas é necessário uma atualização do sistema.

Existe um projeto Open Source, chamado de OpenX1. Esse cliente está disponível tanto para windows quanto para linux. Uma desvantagem desse pacote é que ele não fornece ao usuário muita documentação e a maioria dos servidores linux não provê um pacote para ele.

O sistema operacional IOS, utilizado nos iphone's, suporta o 802.1X desde o lançamento da sua versão 20. No android já é disponível desde o lançamento da versão 1.6 Donut.

Nos sistemas operacionais OS.X, utilizados nos computadores mac's, está disponível desde a versão 10.3

Referencias:

<http://br.ccm.net/contents/786-802-1x-eap>

<http://blogbrasil.comstor.com/bid/398582/O-que-o-protocolo-802-1X>

<http://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan>

<http://www.sj.ifsc.edu.br/~msobral/RCO2/slides/aula12.pdf>

<http://www.vidati.com.br/tag/eapol/>

http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/416/1/CT_GESER_1_2011_14.pdf

