SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GTL 10
14 a 17 Outubro de 2007
Rio de Janeiro - RJ

GRUPO XVI

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS – GTL

PRINCIPAIS ASPECTOS DE SEGURANÇA DE UMA REDE CONVERGENTE

Bruno de Lima Franco (*)

ABB Ltda.

1. RESUMO

Este informe técnico tem como objetivo abordar determinados aspectos das tecnologias baseadas em comutação por pacotes, os principais aspectos envolvidos no conceito de segurança de redes convergentes formadas por equipamentos de transporte e de comutação de camada 2 e uma apresentação de casos de estudo e exemplos.

2. PALAVRAS-CHAVE

Ethernet over SDH, Switch, Layer 2, VLAN, Trunk.

3. INTRODUÇÃO

No XVIII SNPTEE, realizado no ano de 2005 em Curitiba, foi apresentado o trabalho *"Soluções de Redes Corporativas Convergentes para as Concessionárias de Energia Elétrica ("Power Utilities")*, no qual foram identificados os principais aspectos de uma rede operacional de telecomunicações, foi elaborado um comparativo das diversas tecnologias de telecomunicações e foi apresentada como conclusão uma solução convergente baseada na tecnologia "Ethernet over SDH" (EoS), que combina em uma única plataforma, tanto as aplicações *"operacionais*", como as "*corporativas*". Neste último trabalho, também ficou demonstrado que, com o advento do "EoS", a tecnologia SDH deverá permanecer como a mais importante e mais utilizada tecnologia de transporte pelas Concessionárias de Energia Elétrica.

Neste novo trabalho serão abordadas algumas implicações técnicas decorrentes do uso das tecnologias estatísticas como o "Ethernet", "GbE" e o próprio "EoS", bem como serão introduzidos os diversos aspectos de segurança envolvidos em redes convergentes implementadas pelas Concessionárias de Energia Elétrica que utilizem o "EoS" com VLAN's. Por último, serão identificados os principais parâmetros de segurança a serem considerados no planejamento de redes convergentes, de modo a assegurar que as Concessionárias de Energia Elétrica tenham os requisitos básicos das suas aplicações operacionais e os requisitos mínimos de segurança plenamente atendidos, a fim de garantir um fornecimento de energia estável e confiável aos usuários finais.

(*) Av. Monteiro Lobato, 3.411 CEP 07190-904 Guarulhos, SP – Brasil
Tel: (+55 11) 6464-8114 – Fax: (+55 11) 6464-8361 – Email: bruno.franco@br.abb.com

4. PARÂMETROS DE SEGURANÇA NO USO DE VLAN's

Ao se implementar uma rede SDH convergente que utilize uma ou mais VLAN's, diversos parâmetros de segurança devem ser considerados, com o objetivo de, efetivamente, garantir a segurança da rede. Neste trabalho, os seguintes parâmetros serão abordados e avaliados:

4.1. Separação de Tráfego entre segmentos

Conceitualmente, VLAN é um grupo de usuários ou servidores segmentados em redes lógicas distintas independentes da localização física, sendo que cada membro de determinada VLAN possui uma identificação normalmente denominada "Tag". Os diversos tipos de VLAN"s variam de acordo com a tipo de agrupamento lógico de usuários utilizado. Os principais tipos de VLAN's são:

- Agrupamento por porta dos Switches;
- Agrupamento por endereço MAC;
- Agrupamento por protocolo;
- Agrupamento por grupos *multicast;*

A VLAN mais segura é a que utiliza o tipo de agrupamento lógico de usuários por porta, pois há a necessidade de re-configuração do Switch quando ocorrer mudança no local de conexão, um adaptador de rede em modo "promíscuo" não escuta tráfego alheio e eventuais ataques exigem acesso à segurança física ou de configuração dos equipamentos.

4.2. Segurança Física

É recomendável o controle de acesso aos equipamentos SDH, principalmente, em locais remotos e estações sem operadores para que o acesso não autorizado ao rack dos equipamentos seja sempre evitado, sendo que desta maneira, qualquer invasão não autorizada seja sempre facilmente detectada.

4.3. Configuração de Equipamentos

Devem sempre ser criadas senhas de acesso com direitos de acesso claramente definidos. Deve-se dificultar o acesso a portas de console e é recomendável que se criem sub-redes específicas para configuração de equipamentos. Todos os arquivos devem ser cuidadosamente documentados.

4.4. Camada usada na separação de tráfego

Tanto a camada física (Layer 1), como as camadas de enlace (Layer 2) e redes (Layer 3) podem ser utilizadas para a separação do tráfego. Entretanto, a camada de redes (Layer 3) não é muito utilizada em função da sua simplicidade e baixa segurança.

A camada física (Layer 1) e de enlace (Layer 2) são amplamente utilizadas. A utilização da "Camada 1" é, efetivamente, a separação física do tráfego e apresenta a maior segurança possível, embora seja muito radical e dispendiosa na maioria das aplicações.

A camada de enlace (Layer 2) envolve a implementação baseada em Switches e VLAN's, apresenta um elevado índice de segurança e é amplamente utilizado e recomendado por ser o método mais eficiente.

4.5. Possíveis Ataques de Hacker a Redes baseadas em VLAN (Camada 2)

4.5.1. MAC Flooding Attack

Esta não é especificamente uma forma de ataque e sim uma limitação da forma de como a maioria dos Switches trabalha. Cada Switch possui uma tabela interna que armazena endereços de fonte/destino de todos os pacotes. Quanto esta tabela está cheia, novos endereços não podem mais ser amarzenados e o tráfego destinado a estes endereços é, permanentemente, inundado a todos os membros da VLAN de origem. Esta fraqueza pode ser explorada por algum usuário malicioso que queira acionar alguma porta do switch que ele esteja eventualmente conectado. Em Switches não-inteligentes, este problema piora, pois a identidade L2 da fonte não é verificada e, conseqüentemente, é possível que um número ilimitado de dispositivos seja falsificado mediante a falsificação de pacotes.

Para se evitar este tipo de ataque, basta se utilizar Switches que tenham a capacidade de identificar e controlar as identidades de dispositivos conectados e/ou limitarem o número dos endereços do MAC que possam ser usados por uma única porta. Deste modo, a identificação do tráfego de um dispositivo é amarrada diretamente a sua porta de origem.

4.5.2. 802.1Q and ISL Tagging Attack / VLAN's Hopping Attack

4.5.2.1. 802.1Q Tagging

O IEEE 802.1Q é o padrão que possibilita e define o transporte transparente e simultâneo de diferentes VLAN's através de uma única rede física sem perda de informação ou troca indevida entre as diversas VLAN's. Para tanto, cada VLAN é identificada com uma etiqueta denominada "Tag" ("Tagged VLAN") Este canal de comunicação que conecta diferentes Switches e inclui inúmeras VLAN's é denominado um canal do tipo Trunk. Além de incluir diversas VLAN's de usuários, um canal Trunk também deve incluir uma VLAN de Gerenciamento e uma VLAN Nativa, conforme exemplo abaixo:

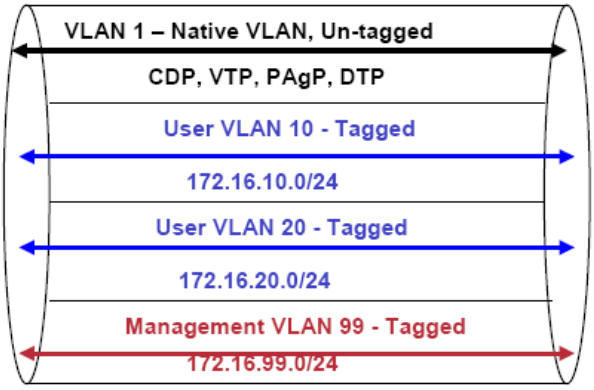

Figura 1 – VLAN Trunk

VLAN 1: Como configuração padrão, todas as portas de um Switch, interfaces de gerenciamento e alguns protocolos de Camada 2, por exemplo, VTP (VLAN Trunking Protocol) ou DTP, precisam ser membros de uma VLAN. Para todas estas funções, a VLAN 1 é escolhida como padrão.

VLAN Nativa: É o termo usado para as interfaces configuradas como VLAN Trunks.

VLAN de Gerenciamento: Deve ser uma VLAN dedicada e totalmente independente das outras VLANS, para que mesmo em caso de problemas na rede, o administrador da rede tenha acesso aos elementos de rede para alterações de configuração e parametrização.

Quando alguma porta do Switch for configurada como Trunk, cada pacote transportado será etiquetado com o número de sua respectiva VLAN e pacotes de todas as VLANS são transportados pelo Trunk contendo o "Tag" 802.1Q, com exceção dos pacotes da VLAN 1. Por definição, pacotes da da VLAN 1 pertencem a VLAN Nativa e são transportados sem etiquetas. Portanto, pacotes pertencentes a VLAN1 ou VLAN Nativa não são alterados ou etiquetados para serem transportados pelo Trunk. Desta maneira, o uso da VLAN Nativa deve ser evitado, pois as informações de identificação dos pacotes e informações adicionais, como classe de serviço, não serão transmitidas.

Os chamados "VLAN's Hopping Attacks" são os esquemas de ataque que permitem que um usuário em uma VLAN comece o acesso desautorizado a uma outra VLAN. Por exemplo, se uma porta do Switch está configurada para dinamicamente estabelecer enlaces do tipo Trunk com outros Switchs, usando o protocolo DTP, ISL ou 802.1Q, e esta porta recebesse um pacote de comando falso, esta porta, indevidamente, se transformaria em uma porta Trunk e começaria a aceitar tráfego destinado a todas as VLAN's, dando acesso indevido a todas as VLAN's.

Este ataque pode ser facilmente impedido, desabilitando nos Switches a opção dinâmica para o estabelecimento de VLAN Trunks. Este modo dinâmico, apesar de facilitar a configuração de redes e switches, é um dos principais pontos de vulnerabilidade e entradas de ataques.

4.5.3. Double-Encapsulated 802.1Q/Nested VLAN Attack

Caso pacotes duplamente encapsulados com o “802.1Q Tagging” forem injetados na rede por algum Switch que eventualmente seja membro da VLAN Nativa do Trunk, a identificação destes pacotes injetados não será preservada, pois pela própria definição de VLAN Nativa, a etiqueta externa será removida e não será transmitida pelo Trunk.. Sendo assim, a etiqueta de identificação interna será a única forma de identificação do pacote. Caso os pacotes sejam duplamente encapsulados com Tags diferentes contendo endereços de VLAN’s distintas, os pacotes poderão ser indevidamente enviados a outras VLAN’s, conforme exemplo abaixo:

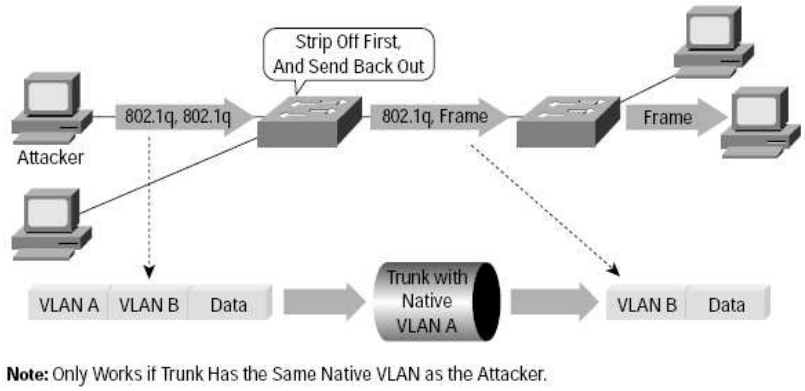

Figura 2 – Double Tag Attack

Apesar de ser efetivamente uma forma de ataque, este cenário pode ser classificado como erro de configuração, uma vez que o padrão 802.1Q recomenda a não utilização de VLAN’s Nativas e recomenda que as VLAN’s Nativas de todos os Trunks sejam apagadas.

4.5.4. ARP Attacks

4.5.4.1. ARP Protocol

Address Resolution Protocol (ARP) é um protocolo para mapear ou associar um endereço IP a um endereço físico (MAC Address) de uma máquina de uma rede local. Uma tabela denomina ARP armazena a correlação entre cada endereço MAC e endereço IP. Este protocolo define as regras para esta correlação e endereçamento. Quando um novo pacote chega ao Switch, o programa ARP identifica o endereço MAC de destino correspondente ao endereço IP para que o pacote possa ser transportado. Caso não seja encontrado nenhum endereço correspondente, o ARP envia um broadcast a todas as máquinas da rede questionando se aquele endereço IP é dela. A máquina detentora do endereço MAC correspondente responde e a tabela é atualizada.

A vulnerabilidade do ARP é que, em princípio, qualquer máquina pode reivindicar que seu endereço MAC está associado a um determinado endereço IP. Isto é possível porque os pedidos/respostas do ARP carregam a informação sobre a identidade L2 (MAC address) e a identidade L3 (IP address) de um dispositivo e não há nenhum mecanismo da verificação da exatidão destas identidades, conforme exemplificado abaixo:

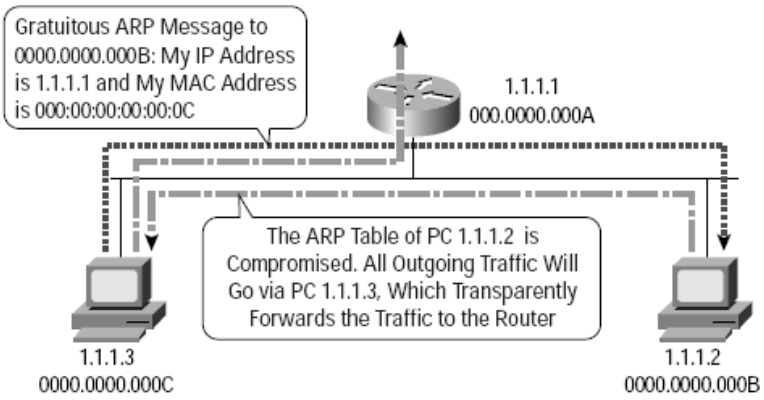

Figura 3 – ARP Attack

É possível previnir este ataque acionando um parâmetro de configuração e de segurança dos Switches, pelo qual é possível especificar a quantidade de endereços MAC o especificar o próprio endereço MAC com permissão para fazer conexão por determinada porta do Switch.

4.5.5. Private VLAN Attack

VLAN's do tipo Privada é uma aplicação de típica de Layer 2 e, conseqüentemente, somente o tráfego L2 é isolado. Se um dispositivo L3 (Router) for conectado a uma porta não isolada de um switch das VLAN's, o tráfego L3 poderá ser enviado a qualquer uma das VLAN's, mesmo que isoladas em L2.

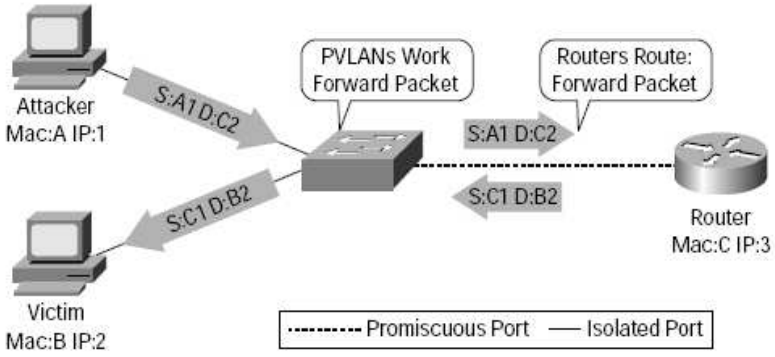

Figura 4 – Private VLAN Attack

4.5.6. Multicast Brute Force Attack

Este ataque tenta explorar as eventuais vulnerabilidades ("Bugs") dos Switches quando a rede é inundada de forma bastante rápida e repetitiva por pacotes do tipo Multicasts. Se o Switch apresentar comportamento indevido, haverá vazamento de pacotes de uma VLAN para outra. Esta técnica de ataque também se verificou ineficiente e os pacotes ficaram limitados aos respectivos domínios de difusão.

4.5.7. Spanning-Tree Attack

Mais uma técnica de ataque que tenta explorar as eventuais vulnerabilidades ("Bugs") dos Switches. Como configuração padrão, o protocolo STP é ativado em todas as portas do Switch que recebem e enviam mensagens STP. A tentativa de ataque foi justamente em conseguir a identificação destas portas que estavam transmitindo mensagens STP e posteriormente falsificar mensagens de que o intruso seria a nova raiz (Root Bridge) na re-configuração do STP. Esta técnica de ataque também se verificou ineficiente e os pacotes ficaram limitados aos respectivos domínios de difusão.

4.5.8. Random Frame Stress Attack

Esta última técnica de ataque consiste em variar diversos parâmetros de pacotes que são constantemente e repetidamente enviados, mantendo-se constante apenas os endereços de destino e origem. Esta técnica de ataque também se verificou ineficiente e os pacotes ficaram limitados aos respectivos domínios de difusão.

4.6. Políticas de Interligação

Como já mencionado neste informe técnico, cada VLAN distinta agrupa usuários e/ou servidores segmentados em redes lógicas distintas e que não se comunicam entre si, mesmo quando conectados a um mesmo Switch.

Para que a interligação de VLAN's distintas possa ser possível, seria necessário o uso de Roteadores ou Switches de Camada 3, porém esta interligação de VLAN's distintas deve ser evitada ao máximo e, se possível, banida a fim de se garantir uma maior segurança ao sistema. Cada VLAN, preferencialmente, deve ter acesso apenas aos seus próprios recursos e os recursos compartilhados, como impressoras e servicores, não devem funcionar como ponte entre VLAN's.

5. SEGURANÇA EM VLAN'S

Conceitualmente, VLAN é um grupo de usuários ou servidores segmentados em redes lógicas distintas independentes da localização física. Cada membro de uma VLAN possui uma identificação normalmente denominada "Tag". Se a identificação dos pacotes de cada VLAN e destes usuários não puder ser alterada após o início da transmissão da fonte e, consistentemente, preservada na comunicação "fim-a-fim", pode-se afirmar que a segurança de uma rede baseada em VLAN é tão confiável quanto à segurança de redes fisicamente distintas.

6. CONCLUSÃO

O uso do Ethernet over SDH (EoS) combinado com VLAN's tem se consolidado como um dos métodos mais simples e seguros no estabelecimento de redes convergentes confiáveis, uma vez que a vulnerabilidade destes sistemas está muito mais relacionada aos erros de configuração e de planejamento de rede, do que às falhas ou deficiências destas tecnologias propriamente dita A tecnologia VLAN tem se consolidado como uma das mais seguras e confiáveis, sendo que a maior, senão a única, vulnerabilidade deste sistema está muito mais relacionada a erros de configuração dos Switches e planejamento de rede, do que a segregação do tráfego por VLAN's propriamente dita. Como acima mencionado, há vários requisitos e parâmetros a serem considerados no planejamento de uma rede SDH convergente que utilize a tecnologia VLAN. Se estes requisitos forem respeitados, a tecnologia VLAN é, suficientemente, confiável para uma combinação segura e flexível dos serviços operativos e corporativos em empresas de energia elétrica.

7. REFERÊNCIAS BIBLIOGRÁFICAS

Research Report: Secure Use of VLANs: An @stake Security Assessment—August 2002, http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf
SAFE: A Security Blueprint for Enterprise Networks, http://www.cisco.com/go/safe/
Best Practices for Catalyst 4500, 5000, and 6500 Series Switch Configuration and Management, http://www.cisco.com/warp/customer/473/103.html
dsniff, by Dug Song, http://monkey.org/~dugsong/dsniff/
VLAN Security Test Report, July 2000, http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
An Ethernet Address Resolution Protocol, RFC 826, http://www.ietf.org/rfc/rfc0826.txt
ARP spoofing attack:
http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm
White Paper: Catalyst 6500 Series Service Provider Feature (Private VLANs), http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm
@stake, http://www.atstake.com/

8. DADOS BIOGRÁFICOS

Bruno de Lima Franco
Nascido em São Paulo, SP em 14 de Novembro de 1977.
Pós-Graduação em Administração de Empresas (2004): FCAV – USP, SP.
Graduação em Engenharia Elétrica (2000): E.E. Mauá, SP.
Empresa: ABB Ltda., desde 2000.
Engenharia de Vendas de Sistemas de Telecomunicações e Teleproteção.