Aluno: André Luiz N. Carneiro RA: 92854

Lista de Exercícios 1 - Princípios de Comunicações

Diego Fiori

ARARAS/SP

04/2021

1) Explique a diferença de WLAN, WMAN, WBAN, WPAN e WWAN (W = Wireless).

A **PAN** é conhecida como Personal area network, uma rede pessoal tendo o bluetooth sendo o mais conhecido e estando mais perto de nós no dia a dia. Ela possui um baixo aspecto em relação a distância chegando no *máximo a 2 metros* nos melhores modelos.

Local area network, também conhecida como **LAN,** normalmente são integradas com redes cabeadas em um ponto de acesso e chegando ao máximo de 150 metros. Caso tenha uma boa propagação nas antenas essa distância pode aumentar.

A **MAN** uma rede metropolitana que trabalha dentro da cidade, podendo atingir até 50km. Já a **WAN** atinge uma área maior, como o próprio nome diz, world area network, atinge uma área muito maior, podendo chegar até 150km.

WBAN - a rede de área corporal sem fio que pode ser incorporado no corpo como implantes. Também pode ser fixada no corpo ou devem ser acompanhadas de dispositivos que podemos carregar de diferentes formas.

2) A tabela abaixo define os nove tipos de serviços dentro de uma agregação wi fi. Explique quais destes estão relacionados com itens relativos à segurança da conexão

Authentication, Deauthentication e Privacy são os serviços relativos à segurança da conexão, pois controlam todo o acesso a rede.

Na 802.11 o authentication envia um quadro de autenticação para o access point contendo a identidade do usuário, para outras formas de autenticação como as de sistema aberto, autenticação de chave compartilhada, a autenticação atua de forma diferente.

Deauthentication é quando é enviado de um lugar onde deseja encerrar a conexão, desautenticando a conexão.

A Privacy no IEEE 802.11 contorna o problema de outros dispositivos poderem ouvir o trafego de informações, fazendo com que aumente o nível de segurança da rede.

3-) Quais são as freqüências ISM?

A Onu criou a seguinte normatiza determinando quatro níveis de frequência do qual no mundo inteiro não precisa de regulamentação, mesmo tendo criado o equipamento, não precisa de autorização de ninguém para opera-lo. Tendo as seguintes frequências que podem ser operadas pelos equipamentos:

902 – 928 MHz (frequência mais utilizada por comunicações de baixa distância e latencia)

2,4 – 2,485 GHz = 2,4 – 2,5 GHz (temos o WI FI trabalhando dessa forma, e também possui outros equipamentos que trabalhavam com essa frequência)

5,475 – 5,775 = 5,4 GHz (WIMAX)

5,795 – 5,875 = 5,8 GHz

4) Qual a diferença de Router Wi Fi e Access Point?

Router Wifi ele fornece o acesso via direcionamento IP (ipv4, ipv6), dividindo a rede e segmentando-a. Tem um link pra fora WAN, que respeita um ip que está pra fora e pra dentro temos uma outra classificação de IP. Possui dois tipos de pacotes, um sendo o Frame, que é enviado ao meio aéreo, tendo o TCP ou UDP que troca informações com entidades e serviços no ambiente de comunicação. Também temos o Beacon que seria o frame enviado em broadcast em todas as entidades com o nome da rede, fazendo a associação com o router wifi.

O acess point já não divide a rede, ele é bridge, nada mais que um ponto de acesso que pede a autorização para outra entidade.

Eles vão propagar um ESSID (nome da rede), que é registrado (podendo ser oculta), que é a identificação de acesso, que não é criptografado.

5) Explique com suas palavras como funciona o sistema de M.I.M.O e em qual padrão ele aparece pela 1° vez?

M.I.M.O (Minimun input Minimun output) ou popularmente conhecido como múltiplas entradas e saídas múltiplas, ele apareceu pela primeira vez no 802.11g e pode ter variações dependendo dos locais, como por exemplo um lugar fechado, que deriva de oscilações,

podemos fazer modulações de M.I.M.O para adaptar-se no local adequadamente, sendo muito pouco explorado por muitos técnicos.

Também é conhecido pela utilização de várias antenas no transmissor e no receptor, sendo uma tecnologia econômica que oferece vantagens substanciais para tornar os links sem fio de 1 Gb/s uma realidade.

6) O que é o padrão IEEE 802.11 ac?

É o padrão que chega em 1 Gig/seg com variações de 500mb/s, tendo o conceito de explorar dois host's em um só, podendo aumentar o link de acesso. Possui uma frequência de 5.8 Ghz se caso venha a ser utilizado unicamente, também possui convergência, podendo conversar com os demais sendo IEEE o equipamento.

A transmissão de banda é configurável, influenciando o corte que vai ter no espectro, quantos canais terá, se será 20/40/80. Podendo alterar também a modulação, do qual melhora a condição de link/onda.

Possui FEC coding, tendo umas opções de convolução e sendo opcional. M.I.M.O sendo ligado em relação ao ambiente, podendo usar várias antenas para replicar, uma sendo de transmissão outra de recepção, sempre explorando o equipamento para o melhor perfomance, chegando em até oito tipos de alterações.

7) Quantos canais possuem a IEEE 802.11 b/g/n? e quais canais devem ser evitados?

A IEEE 802.11 tem 11 channels e por default vem com o channel 6 ou 11, e vindo como padrão deve ser evitado pendurar todo mundo em um só channel, para evitar a interferência. Temos como maior eficácia trabalhar com os canais mais elevados, entre 6 e 11, encaixando 7 8 9 10 teria um throughput maior.

8) Qual o nome que os enlaçamentos 1:1 e 1:n recebem para IEEE 802.11?

O mais simples é o Ad Hoc, 1:1, utilizado em bluetooth. O mais comum que se usa é o padrão de infra, que distribui em broadcast as informações, 1:n.

9) Explique como funciona um simples ponto de acesso rogue.

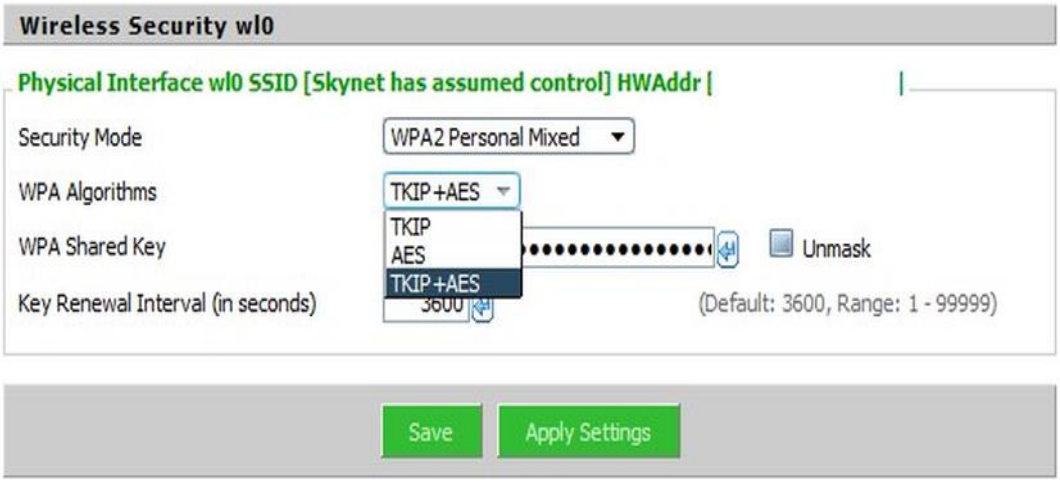
Um acesso rogue um atacante instala de uma forma oculta e sem autorização um Acess Point em um ponto fixo da rede, e dessa forma ele captura informações acessando o AP.

10) Qual a diferença da criptografia WPA Enterprise e Personal em IEEE 802.11?

A maior diferença entre ambos, são os tipos de criptografia que são usados.

O Personal é o WPA puro, também conhecido como a versão “doméstica do wpa”, utilizasse o WPA-PSK, pre-shared key, os usuários podem ter o modo de chave pré compartilhada.

Possui uma encriptação TKIP (também pode altera-la para AES, TKIP + AES, TKIP), do qual para ataca-la com essa encriptação, os atacantes devem utilizar umas ferramentas mais avançadas de hacking.



Enterprise tem um risco menor apesar de ser utilizado para uma estrutura mais complexa, e é ligado no servidor RADIUS do qual controla toda a autenticação. O servidor RADIUS pode ser tanto uma máquina Linux (com o FreeRADIUS) quanto um servidor Windows, cujo endereço é indicado na configuração do access point.