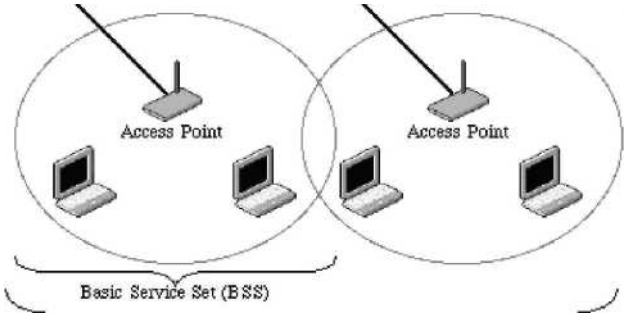
DisttUmtinn



Extendei Semce Set(ESS)

Ad-hoc režim (nazývaný též peer-to-peer režim nebo Independent Basic Service Set (IBSS)) je množinou 802.11 bezdrátových stanic, které komunikují pQmo mezi sebou bez použití postupového bodu nebo drátové sítD Tento režim je užitéQiý pro rychlé a jednoduché nastavení bezdrátové sítěkdekoliv, kde neexistuje bezdrátová infrastruktura nebo kde není potBbná (hotelový pokoj, letištQ.

4.5. CojeBSSID?

Šesti-bytová adresa, která odlišuje pHlstupový bod od ostatních. Taky známa jako SSID. Poskytuje síttvé ID nebo jméno.

4.6. CojeESSID?

Extended Service Set ID (ESSID) je název sítQ ke které chcete p [Ustupovat. Je použita pro identifikaci rozlišných bezdrátových sítí.

4.7. Co může způsobovat interferenci?

Zdroje rušení:

- PHkážky: stQiy, stropy, nábytek..

Stavebný materiál: kovové dveB, hliníkové plochy. Elektrické za
[Uzení: mikro vlnky, monitory, elektrické motori. ZpCsoby omezení
rušení:

- Minimalizace po Qu sten a strop ů
  Anténu umístit na nej vhodn *Q* ší místo
  Udržovat bezdrátové za Slzení od elektrických spotHbiDD (mikrovlnek, monitor ů elektrických motorp)
  PQdat další p Hstupový bod, když je to nevyhnutný

4.8. Co je autentizace Otevřený systém a Sdílený klín?

IEEE 802.11 podporuje dva podtypy síttvé autentizace: otevBný systém a sdílený klíD V OtevBnom systému nemCže žádná stanice žádat autentizaci. Stanice, která potHbuje být autentizováná s jinou bezdrátovou stanicí posila Udící rámec, který obsahuje identitu vysílající stanice. PQjímací stanice vrací rámec, který indikuje zda byla vysílající stanice rozpoznána. PQ autentizaci pomocí sdílených klín pkaždá bezdrátová stanice obdrží tajný sdílený klip pEes bezpeQiý kanál nezávislý od kanálu definovaných 802.11.

4.9. CojeWEP?

Funkce IEEE 802.11, která ponuka vysílání rámcD sbezpeChostí podobné drátové sítí. Aires Equivalent Privacy generuje tajný sdílený šifrovací klip ktorý vlastní vysílejíci i pQjímací prvek. Používá se jako základní zabezpečení pBd nabouráním Vaši sítD Je však velmi lehce pEslomitelná.

WEP se spoléhá na tajný klip který sdílejí pQjjímací stanice a pQlstupový bod. KlíDšifruje

pakety pBd tím než jsou vyslány. Kontrola integrity se používá pro zjištChí, zda pakety nebyli modifikovány v prCbChu pBnosu.

4.10. Co je Threshold rámce ?

Protokol používající fragmentaci ráme ů definovanou IEEE 802.11, který se používá pro dosáhnutí paralelního vysílaní. Velké datové rámce se rozkládají do vícero Qstí, každá má velkost podle rámce threshold. Zapnutím threshold rámce m ůžeme mChit velikost rámce. UrCením vhodné velikosti rámce je velmi ddežité. Když je rámec moc malý, informace je rozlezena do mnoha Části a nároChDa zdlouhavDse spravovává. Naopak, když je rámec moc velký, jeho obnova pCJ ztrátDmCže být zdlouhavá a tým se zpomalí celkový pEsnos. Proto je nutné zvolit pQtaiDéliou velikost rámce.

Rámec threshold je maximální velikost paketu použitého pCJ fragmentaci. Všechny vCtší pakety budou fragmentovány.

4.11. CojeRTS?

Request to Send threshold je velikost paketu, kterého pBnos je Oken RTS/CTS transakci. IEEE 802.11-1997 povoluje krátkým paketQn, aby byli vysílány bez RTS/CTS transakcí. Každá stanice mCže mít rozliChý RTS trashold. RTS/CTS je použita když naroste velikost datového paketu definována RTS trashold. Spolu s CSMA/CA mechanizmem, vysílací stanice vysílá RTS paket pBjímací stanici a aká na CTS (Clar to Send) odpovDDod p [zjímající stanice, pBd tím než se pošle samotný datový paket.

Toto nastavení je užiteChý pro sítDs velikým množstvem klientP Když bude v síti mnoho klient ů a vysokými požadavky na siť vznikne mnoho kolizí. Snížením RTS threshold, bude ménDkolizí a provoz by sem mCl zlepšit. S rychlejším RTS se systém mCže rychleji zotavit. RTS pakety samozBjmDzabírají šíCku pásma, takže když nastavíme RTS pílíš nízko, celková rychlost sítDse zpomalí.

4.12. Co je interval Beacon ?

V závislosti na datových rámcích, které nesou informaci pro vyšší vrstvy, 802.11 zahrnuje management a kontrolní rámce, které podporují pBnos dat. Beacon rámec, co je typ CMcího rámce, povoluje stanicím aby nadvázali a udržovali komunikaci podle dohodnutých pravidel.

Beacon internval representuje Časový interval mezi vysíláním beacon. PBd tím než stanice vstoupí do úsporného režimu, stanice potBbuje interval beacon, aby vQiCla kdy se má probudit (a taky vQiel jestli jsou na pCOstupovém bode nazhromaždený rámce).

4.13. Co je to typ preambule ?

Jsou dva typy preambule definované IEEE 802.11 specifikaci. Dlouhá preambule potBbuje více Času, aby byla dekodérem zpracována. Všechny 802.11 za Slzení

podporujou dlouhou preambuli. Krátká preambule je navržena pro zlepšení výkonu (pro VoIP systémy). Rozdíl mezi preambulemi je v tom, že dlouhá má 128 bitDa krátká 56 bitD

4.14. Co je vysílání SSID?

Vysílání SSID je daný v pEOstupových bodech beaconem. Oznamuje Váš pHstupový bod okolnímu bezdrátovému svCtu. Zakázáním této vlastnosti, SSID nakonfigurováno v klientovi musí souhlasit s SSID pQlstupového bodu.

NCkteré bezdrátové zaQkení nemohou pracovat správnQ když SSID není vysíláno. Pokud Vaše zaQkení pracuje bez potHby zapnutého SSID vysílaní, je dobré z bezpečnostního pohledu toto nastavení zachovat. Není to však náhrada za WEP, blokaci MAC nebo jiné zpCsoby zabezpD Ěhí.

4.15. Co je WPA (Wi-Fi Proteced Access) ?

WEP je nedostatečný zpCsob zabezpečení bezdrátové sítD Proto bylo vyvinuto WPA, které poskytuje vyšší úroveD zabezpečení. Pracuje na jiném principu jako WEP a je nároQiEjší ho pBlomit.

4.16. CojeWPA2?

Druha generace WPA. Je založena na standartu 802.11 i. Založená na algoritme AES. Zatím nebyla pBlomená.

4.17. Co je autentizace 802.1x?

ZabezpeQije autentizaci na úrovni MAC. Definuje protokol EAP (Extensible Authentication Protocol) over LAN (WAPOL).

4.18. Co je TKIP (Temporal Key Integrity Protocol) ?

TKIP je souastí 802.1 1i šifrovací standart pro LAN. TKIP je další generaci WEP, který zabezpeQije bezdrátovou síD TKIP poskytuje integritu zprávy, mechanizmus obnovení klín □

4.19. Co je AES (Advanced Encryption Standart) ?

Symetrický šifrovací algoritmus, který využívá WPA2.

4.20. Co je IAPP (Inter-Access Point Protocol) ?

IAPP podporuje povoluje roaming bezdrátových stanic v podsíti IP.

IAPP definuje zprávy a data, aby byli vymQiQié mezi pEOstupovým bodem a mezi IAPP a vyššími vrstvami Qldících entit, aby podporovali roaming. Protokol IAPP používá TCP pro komunikaci pQlstupového bodu a UDP pro RÁDIUS žádost/odpovDDvýmQiu. Taky používá rámce druhý vrstvy pro update smQovacích tabulek za Slzení druhé vrstvy.

4.21. Co je WDS (Wireless Distribution Systém) ?

WDS umožQije pQlstupovým bodQn komunikovat bezdrátovDpQmo s AP jako pQ režimu wireless bridže nebo repeater.

4.22. Co je uPNP (Universal Plug and Play) ?

UPnP je otevBná síQvá architektura, která pozostáva ze služeb, zafllzení a kontrolních bodQ Cílem je umožnit datovou komunikaci pBs UPnP zaQkení bez kontroly media, operaQiího systému, programovacího jazyku a drátových/bezdrátových p Opojení.

4.23. Co je velikost MTU (Maximum Plug And Play) ?

MTU indikuje každý paket v zásobníku. Když je jeho velikost v mší než nastavená velikost, dochází pBd jeho vylaním k fragmentaci. MTU PPP pOpojení je nastaveno

menší než MRU peera. Defaultní adresa je 1400.

4.24. Co je klonování MAC adresy?

Klonování MAC adres je navrženo pro speciální klienty, kteO potBbují registrovat MAC adresu pro poskytnutí služeb.
Vzhledem na to, že všichni klienti komunikujou pHs pOstupový bod, požadovaná adresa se nastaví na postupovém bodD

4.25. CojeDDNS?

DDNS je zkratka Dynamic Domain Name Server. Je navržena když se uživateli dynamicky mQií IP adresa a potHbuje, aby DNS adresa zCstala stejná.

4.26. Co je NTP klient?

Slouží pro získaní pSsného Qsu pBs Internet. Uživatel nastaví adekvátní Qsovou zónu, NTP server a IP adresu.

4.27. CojeVPN?

VPN je zkratka Virtual Private Network. Je navržena pro vytváBní soukromé sítD veBjnou sítí Internetu.

4.28. CojeIPSEC?

Je to zkratka pro IP Security. Používá se pro bezpeQiý transport dat pSs VPN.