Je kent het wel. Je bent op een grote bijeenkomst, een congres of iets dergelijks, en iedereen blijft maar klagen over de WiFi. Maar de keiharde waarheid is: er is meestal helemaal niks mis met de WiFi.

Terwijl er een compleet boekwerk kan worden geschreven over specifieke WiFi-installatieopties die problemen kunnen opleveren, zoals te veel of te weinig AP's, onjuiste kanaalinstellingen, slordig geplaatste AP's of te veel SSID's, wordt er gewoonlijk ook geklaagd als juist al die installatievalkuilen netjes zijn vermeden.

Hier zijn de meest voorkomende oorzaken die WiFi maken tot ieders meest favoriete gespreksonderwerp, meer nog dan het weer - dat ook al nooit goed is.

Meer breedband alstublieft

Het meest voorkomende en meest duidelijke probleem waarvoor WiFi wordt vervloekt zijn waardeloze of trage breedbandverbindingen. De bedoeling van de meeste WiFi-netwerken is om lokale verbindingen met het internet te bieden. WiFi kan tegenwoordig verbindingen bieden met snelheden van honderden megabits per seconde, maar komt haast tot stilstand als er niet genoeg backhaul met het internet is. Zelfs een 100 Mbps-verbinding is te traag als je duizenden clients moet bedienen met een dozijn AP's die zowat een gigabit snelheid aankunnen. Dat maakt dat WiFi traag of onbetrouwbaar lijkt.

Een ander groot probleem, dat niet direct is gerelateerd aan WiFi, is simpelweg een slecht ontwerp van het kabelnetwerk. Switching, routing en functies als DHCP en DNS-systemen die niet goed zijn geconfigureerd om de explosie aan WiFi-netwerkverbindingen aan te kunnen, kunnen het netwerk storen en onderwijl krijgt WiFi de schuld van dat probleem.

De gebruikers blijven plakken

Er zijn verschillende manieren waarop het niet juist opzetten van DHCP problemen veroorzaakt die de meeste mensen wijten aan de WiFi. De Dynamic Host Configuration Protocol (DHCP) is een methode om automatisch de TCP/IP-netwerkinstellingen op computers, printers en andere netwerkapparatuur te configureren.

Een bekend probleem met DHCP is een te lange DHCP-lease. Dat is de tijdsduur dat een apparaat een IP-adres mag bezetten. In een standaard netwerkconfiguratie kan die periode uren of zelfs dagen duren. Actieve apparaten wordt steeds gevraagd door de DHCP-server om de lease te vernieuwen wanneer de toegestane tijd half is opgebruikt. Een inactief apparaat verliest simpelweg zijn lease en het adres wordt dan vrijgegeven en aan een ander apparaat toegewezen.

In een druk bezet netwerk is het mogelijk dat na een tijdje de IP-adressen op raken. Mocht de lease te lang duren, heeft de DHCP-server op een gegeven moment geen adressen meer om toe te wijzen, wat bij de gebruiker overkomt alsof de WiFi het heeft begeven. Kortere leases geven wel wat meer verkeer door de toenemende vernieuwingen, maar dat is het waard als je geen tekort wil aan vrije IP-adressen.

Een (ver)taalprobleem

Een domain name server (DNS) is een onmisbaar onderdeel van elk netwerk. Als een apparaat wil weten welk adres het moet gebruiken voor voorbijkomend verkeer geeft de DNS-server een vertaling van de naam (of URL) naar een IP-adres.

Als een DNS-server het niet meer aankan, in een druk bezette WiFi-omgeving bijvoorbeeld, kan het niet meer zijn rol vervullen als vertaler van adressen, bijvoorbeeld als er meer apparaten verbonden zijn dan zijn rekenkracht aankan. En als een DNS-server crasht of als clients de server niet kunnen bereiken, houdt het voor die gebruikers helemaal op. Dat betekent dat het verkeer slechts sporadisch verder kan en wordt de indruk gegeven dat het WiFi-netwerk overbelast is ondanks dat elke client op een juiste manier verbonden is.

DNS-redundantie is in dit geval een helpende oplossing, vooral als er veel concurrerende WiFi-netwerken zijn. Een goed doordacht netwerk heeft redundantie ingebouwd en heeft meerdere DNS-servers om grote aantallen gebruikers aan te kunnen.

De Big MAC-aanval

Elk aparaat heeft een uniek media access control (MAC)-adres dat wordt gebruikt door netwerkswitches om verkeer rond te leiden. Verschillende soorten switches hebben verschillende limieten op het aantal MAC-adressen die ze kunnen volgen.

Een core switch heeft in de regel een grote MAC-tabel dat het in staat stelt veel apparaten te volgen, terwijl een switch aan de buitenkant van het netwerk strakkere tabelgrenzen kent. Wanneer die grenzen zijn bereikt verliest de switch zijn vermogen om op een juiste manier verkeer door te sturen naar waar het heen zou moeten en daardoor overspoelt het alle poorten in een poging het juiste pad te vinden. Als dit gebeurt zijn er eigenlijk al flinke hoeveelheden verkeer doorgestuurd en dat resulteert in pakketjes die worden gedropt en niet zo'n klein beetje ook.

Als grote aantallen apparaten tegelijkertijd proberen het netwerk op te komen, worden de DHCP-requests en de ARP's (adress resolution protocol) belast en zien we opnieuw het probleem dat het lijkt alsof de WiFi brak is terwijl er helemaal niks met de WiFi zelf aan de hand is.

Een wat meer verborgen limiet dan het aantal MAC-adressen dat een switch aankan, is het aantal dat het aankan op een virtuele LAN of subnet. Een WLAN voor gasttoegang is over het algemeen geconfigureerd voor één VLAN. Maar de edge switches hebben vaak een lagere limiet voor het aantal MAC-adressen per VLAN dan voor de totale switch.

Het netwerk voor gasten tijdens een event met heel veel bezoekers is over het algemeen geconfigureerd voor één VLAN. In dit geval ziet elke switch aan de rand van het netwerk elk MAC-adres van elke gast die aan het netwerk hangt. Daardoor wordt al snel de limiet bereikt bij die switches voor een enkele VLAN. Door de switches goed in te regelen en waar mogelijk meerdere VLAN's te gebruiken, of het verkeer tunnelen naar de sterkere core switches, zal het probleem kunnen worden verholpen.

En dan nu: broadcasting

.Wanneer broadcast (UDP)-pakketjes door een apparaat worden verzonden via WiFi, gaat dat over een veel lagere snelheid dan in het geval ze direct worden verzonden naar een ontvanger (webserver, VPN, etc). Broadcast-verkeer heeft geen voorkennis en krijgt geen bevestiging. Dat betekent dat het apparaat niet altijd weet of het pakketje wel aankomt. Broadcast-pakketjes worden om die reden altijd meerdere malen verzonden.

Het gevolg is dat broadcasts meer tijd pakt dan unicast (TCP)-verkeer. Omdat WiFi een gedeeld medium is waar gebruikers strijden om toegang en wachten op beschikbaarheid van het netwerk voordat ze verkeer kunnen verzenden en ontvangen, kan een teveel aan broadcast het netwerk onderuit halen. Maar bepaalde soorten broadcasts, zoals DHCP-requests en ARP's zijn nu eenmaal nodig. Dus het simpelweg uitschakelen van broadcasts is geen optie.

Een goed netwerkontwerp zal altijd broadcasts mogelijk maken, maar zet daar zoveel als mogelijk een rem op. Een groot Layer 2-netwerk, dat het meest voorkomt tijdens events als een handelsbeurs of een voetbalwedstrijd, is een perfecte kans voor broadcasts om het netwerk de nek om te draaien. Apparaten zien elkaars broadcasts - of ze het nu nodig hebben of niet. Nog erger: als het verkeer bestaat uit broadcasts, is het verzenden van echte data door andere apparaten niet mogelijk.

Te veel broadcasts binnen een kabelnetwerk is net zo dodelijk als te veel broadcasts door de lucht. Het resultaat lijkt op een overbelast WiFi-netwerk, maar dat is helemaal niet het geval. Pakketjes worden gedropt bij de switches op het moment dat een pakketjes-per-secondegrens is bereikt. Bij WiFi kan het isoleren van clients het effect verminderen en tevens beveiliging geven aan de draadloze apparaten. Het is ook nodig om de broadcasts in de hand te houden aan de kant van het netwerk binnen de switches door VLAN's te gebruiken om het aantal broadcasts-domeinen binnen de perken te houden. Switches die VLAN's toestaan om dynamisch te worden toegewezen aan een enkele apparaat of een groep apparaten tegelijk zal dat probleem oplossen.

Conclusie: WiFi krijgt vaak onverdiend de schuld. Ja, WiFi is niet perfect, maar het is tevens afhankelijk van het bekabelde netwerk dat alles verbindt en kan nooit zijn capaciteiten overstijgen. Hoewel we alleen oppervlakkig de vele uitdagingen van WiFi hebben belicht die niet WiFi-gerelateerd zijn, hopen we wel dat de beschreven valkuilen ervoor zorgen dat de notoire WiFi-critici de zaken eens wat meer in perspectief zien.