Aerohive NETWORKS

Whitepaper

BYOD och mer därtill:

Öka produktiviteten med BYOD

Mobilitet, produktivitet och BYOD (bring your own device)

Mobilitet är en av de drivande faktorerna i dagens teknik. För bara några år sedan var trådlösa anslutningsmöjligheter en bekvämlighet för konferensdeltagare och elever som ville sitta utomhus när de skrev sina examensarbeten. Nu används trådlösa enheter överallt. Trådlös mobilitet ses inte längre som en bekvämlighet, utan snarare som det vanligaste sättet att ansluta till ett nätverk. Det är länge sedan en nätverksadministratör kunde sitta och planera tre Ethernetportar per användare, och sedan basera switchar, åtkomst och kapacitet på det. Nu ansluter inte användarna bara sina företagsdatorer utan även olika privata och företagsdistribuerade enheter. Jobbet har förvandlats från en fysisk arbetsplats till något man gör – när som helst, var som helst och med vilken enhet som helst. I en undersökning svarade fler än 80 procent av arbetstagarna att de tar med sig privata enheter till jobbet – och 87 procent av dem använder enheterna till arbetsrelaterade aktiviteter (och inte bara till Facebook!).[1]

Under 2011 rapporterade IDC att fler enheter levererades utan Ethernetportar än med, vilket aldrig hade hänt tidigare.[2] Samtidigt som vi förbereder oss för alla dessa trådlösa enheter på arbetsplatsen står it-administratörerna inför fler utmaningar än någonsin tidigare. Hur stor bandbredd behövs? Vilka typer av enheter kommer att dyka upp? Idag verkar det som att 72 procent av alla privata enheter är Apple-produkter[3] – men hur blir det nästa år? Hur kan en it-administratör förbereda sig och använda samma resurser när de inte vet hur många enheter det gäller, vilken bandbredd som behövs och vilka anslutningskrav som finns? Hur kan administratören vara säker på att nätverket är säkert, högpresterande och redo för nästa våg av ny teknik?

Det här är problemet med BYOD. Fördelen med att låta användarna ta med sig sina privata enheter till jobbet är att produktiviteten och mobiliteten ökar. Till nackdelarna hör den ökade oron för att enheterna inte ska vara säkra, att personalen ska distraheras av programmen snarare än att använda dem i arbetet och, framför allt, att it-personalens arbetsbörda ska öka eftersom de måste hantera support och problemlösning för enheterna.

Något som många inte tänker på med BYOD är att det gäller inte bara att ansluta användarna till nätverket, det gäller även att hantera deras enheter när de väl är anslutna. Det blir något av en chansning att ansluta mobila och privata enheter till nätverket. Ett av de första kraven för en nätverksadministratör som utvärderar lösningar från nätverksleverantörer borde vara att det finns ett säkert sätt att ansluta och övervaka hanterade och ohanterade enheter. Men vad gör man med dem när de har anslutits till nätverket? Vilka funktioner ska man leta efter för att garantera säkerhet, integritet och produktivitet när användarna har tillåtits att ansluta sina enheter? Det som tar upp it-avdelningens tid är inte att ansluta enheterna till nätverket – det är att hantera enheterna när de har anslutits. För att lyckas med BYOD måste man kunna köra rapporter om normsäkring och ge användarna tillgång till relevanta tjänster och resurser utan att ge dem tillgång till sådant som de inte har behörighet till. Enheterna får inte heller öka belastningen på nätverksresurserna.

I det här dokumentet går vi igenom viktiga krav för anslutning och produktivitet så att du kan se till att ditt nätverk verkligen är redo för den mobila explosionen. Här finns en översikt av alternativ för den åtkomst, autentisering och säkerhet som behövs samt information om hur du kan förbereda nätverket så att alla enheter som ansluts till det är kompatibla och produktiva.

---

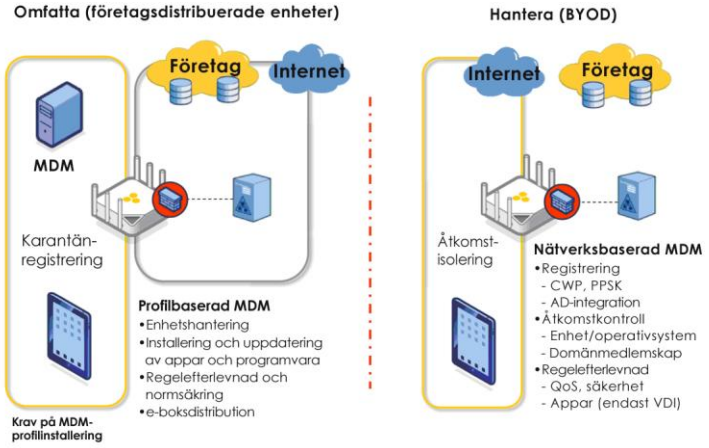
[1] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals", Dell KACE 2011

[2] IDC, "Market Analysis Perspective (MAP) Enterprise Communications Infrastructure Market" 2010

[3] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals" 2011

Ansluta användare till nätverket

En av de första utmaningarna för administratörerna är att definiera exakt vilka enheter som kan klassas som BYOD. BYOD används ofta felaktigt för att beskriva alla konsumentenheter som kan anslutas till företagsnätverket. I verkligheten innebär BYOD en privat enhet som slutanvändaren äger och ansluter till nätverket utan att den har distribuerats av it-avdelningen. Det finns eventuellt ett parallellt initiativ som nätverksadministratörer måste ta hänsyn till. Vissa it-avdelningar vill införa konsumentprodukter som bl.a. surfplattor för att sänka hårdvarukostnaderna och öka produktiviteten i specifika användningsområden som t.ex. i mindre butiker eller för elektroniska läkarjournaler. Konsumentanpassningen av it kräver även en kunskap om nätverk för att kunna dra nytta av de kostnadsbesparingar och den flexibilitet som sådana enheter ger. Samtidigt måste det gå att kontrollera exakt hur enheterna används i nätverket. En omfattande lösning för mobila enheter måste ta hänsyn till både konsumentanpassningen av it och BYOD för att kunna stödja, hantera och omfatta de olika enhets- och klient typer.



Det finns två huvudsakliga ståndpunkter när det gäller att ansluta mobila enheter till nätverket på ett säkert sätt. Många företag använder agentbaserade MDM-lösningar (Mobile Device Management). På så sätt kan de vara säkra på att de anslutna enheterna har rätt mjukvara, behörighet och säkerhetsinställningar innan de släpps in i nätverket. Dessa agentbaserade lösningar är mycket populära bland större företag och skolor, särskilt bland dem som försöker införa fler konsumentprodukter och som hanterar många företagsägda eller skolägda mobila enheter. Ett annat alternativ är nätverksbaserad MDM. Där installeras inte någon agent på klientenheten, utan nätverksenheterna är istället smarta nog att själva klara klassificeringen baserat på användaridentitet, enhetstyp, plats och tid. För att kunna skapa en riktigt omfattande infrastruktur för BYOD och mobila enheter, måste du kunna stödja både agentbaserad och nätverksbaserad MDM. Då kan du använda och kontrollera konsumentenheterna inom företaget och samtidigt ge stöd till de användare som inte vill installera en agentbaserad lösning på sina privata enheter. Det betyder att nätverksenheterna måste vara ännu smartare så att administratörerna antingen kan kräva att agenter installeras eller klassificera användare och enheter och sedan använda åtkomstkontroll för att garantera att de privata enheterna används på ett säkert och produktivt sätt i nätverket.

Aerohive har i synnerhet fokuserat på en smart infrastruktur som kan hantera explosionen av mobila enheter. Vi kan erbjuda flera funktioner för att se till att enheterna ansluts på rätt sätt till nätverket. I HiveOS, operativsystemet som driver alla Aerohive-enheter, finns funktioner som t.ex. registreringskarantän och -krav för agenter, nätverksbaserad MDM, inbyggda "stateful firewalls" i alla accesspunkter samt GRE-tunnlar, som i kombination kan hjälpa dig att lyckas med BYOD-strategin.

HiveOS har inbyggd redundans, är motståndskraftigt och framtidssäkert, tack vare att vi använder gränsbaserad information och Cooperative Control för att garantera klientanslutningarna. En enstaka

Aerohive-accesspunkt klarar alla beslut om vidarebefordring, säkerhetskrav och avancerade funktioner som du kan läsa om nedan, men det är när den kopplas ihop i en "hive" av enheter som Aerohive-systemet blir riktigt kraftfullt. Med Aerohive Cooperative Control kan du inte bara tillhandahålla säker kabelansluten eller trådlös åtkomst, du kan även använda MDM-funktioner för att se till att de privata enheterna ansluts till rätt resurser med utgång från alla associerade uppgifter, t.ex. identitet, enhetstyp och plats. Då kan den privata enheten användas för att öka produktiviteten istället för att slösa resurser.

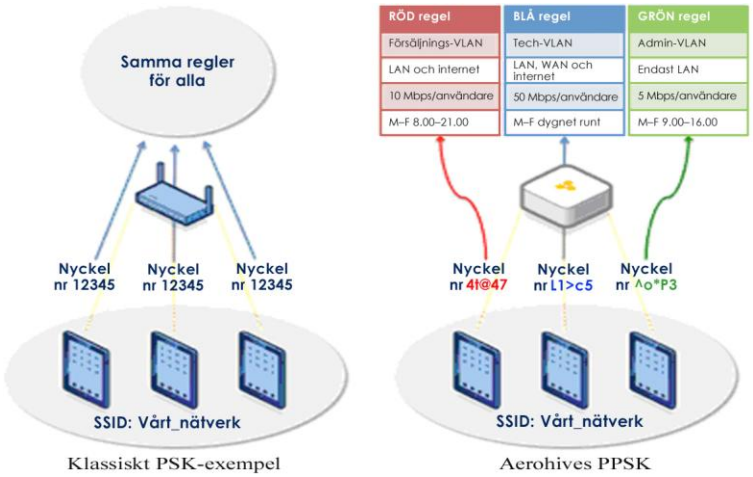
Autentisering och åtkomst

En av de största utmaningarna med att kunna garantera säker åtkomst med privata enheter är att de här enheterna har tagits fram för att enkelt kunna anslutas till alla typer av nätverk – även de som kräver certifikat. Det är dessutom lika viktigt att ha stöd för äldre enheter som bara har stöd för gamla nätverk som 802.11g och som inte klarar certifikatbaserad autentisering. Med Aerohives lösning får administratören många olika alternativ att ansluta användarna till nätverket på ett säkert sätt.

En av de vanligaste säkra nätverkstyperna är att konfigurera WPA2-Enterprise (802.1X) på företagets SSID. Då krävs minst en kombination av användarnamn och lösenord samt att servercertifikatet godkänns för att autentiseringen ska genomföras. Om inte en administratör tar till extrema åtgärder och kräver att alla enheter som ansluts till nätverket har ett installerat certifikat (vilket skulle vara en stor administrativ uppgift och i vissa fall omöjligt att genomföra) är det mycket lätt att ansluta till ett nätverk på moderna mobila enheter. Man behöver bara klicka på godkännandeknappen och ange inloggningsuppgifter för att ansluta en privat enhet till den här typen av säkert nätverk. Administratören har kanske en säker autentiseringsmetod i det här läget men vem vet vad de här enheterna sysslar med i nätverket? Läs mer i avsnittet om säkerhet och regelefterlevnad nedan för information om hur du kontrollerar detta.

Även innan enheterna ansluts till nätverket finns det flera andra alternativ som Aerohive har tagit fram för att lösa problemet med att ansluta användare på ett säkert sätt. Utöver det vanliga öppna gäst-SSID:t med en landningssida med villkor, låter Aerohive dig autentisera användarna som ansluts till något SSID (öppet eller nyckellåst) mot en webbportal som kan knytas till Active Directory (eller någon annan katalogserver). Du kan till och med kräva MAC-autentisering så att endast vissa enheter eller enhetstyper kan anslutas till nätverket.

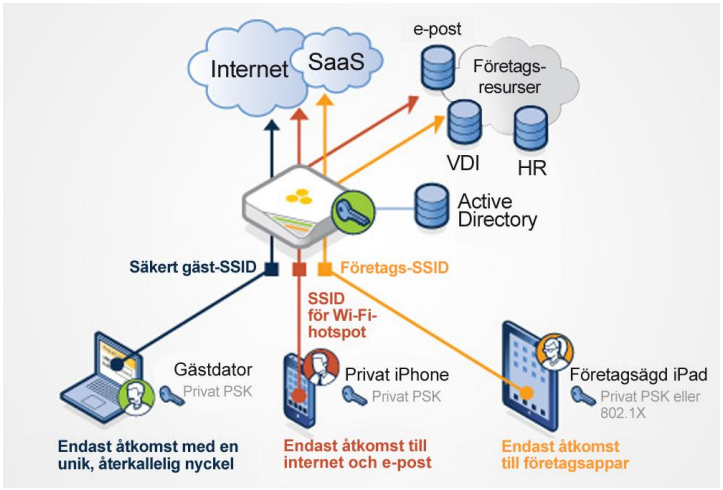
En annan unik Aerohive-funktion är vårt patentsökta PPSK-system (Private Pre-Shared Key). Funktionen är väldigt praktisk eftersom administratören kan utfärda behörighet efter användare eller enhet, men de användare som vill ansluta till nätverket behöver varken certifikat eller inloggningsuppgifter. Administratören kan ange en särskild nyckel eller nyckelgrupp som har definierad nätverksbehörighet, som t.ex. tilldelat VLAN, brandväggsregler och tunnelrättigheter, och kan även knyta nyckeln till den första enheten som ansluts så att inga andra privata enheter kan anslutas med samma nyckel. Den här enkla lösningen ger all den enhetskryptering och -säkerhet som normalt förknippas med mer komplexa 802.1X-lösningar men den fungerar på alla enheter som har stöd för PSK utan att några certifikat krävs.



Säkerhet och regelefterlevnad

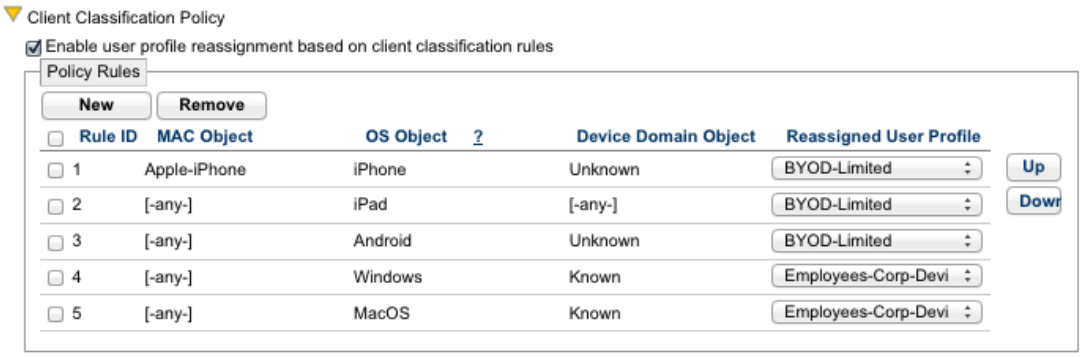
När administratören har fastställt en autentiserings- och åtkomstmetod är nästa steg att se till att de anslutna enheterna följer riktlinjerna för nätverket, baserat på uppgifter som t.ex. identitet, enhet, plats och tid.

Som en del av Aerohives regelefterlevna tilldelas en användarprofil till den anslutna enheten. En Aerohive-användarprofil definierar behörigheten till nätverket, t.ex. vilket VLAN som användaren ska tilldelas, brandväggs-, tunnel- och QoS-regler för användaren eller användargruppen, klientkravsfunktioner som bl.a. SLA och klientklassificeringsinställningar och många andra inställningar som kan tillämpas beroende på användare. Huruvida det går att definiera hur användarprofilerna används beror på vilken typ av autentisering som har definierats samt vilka klientklassificeringsregler som har konfigurerats.



Med klientklassificering kan administratören införa fullständig nätverksbaserad MDM med några få klick. Nätverksbaserad MDM (NMDM) innebär att enheterna som ger tillgång till nätverket, t.ex. accesspunkterna, switcharna och routrarna, kontrollerar regelefterlevnaden utan att en agent måste installeras på klienten. Du kan styra vilka klienter som stöds och hur många klienter en enstaka användare kan ansluta till nätverket, utan att oroa dig för installations- eller kompatibilitetsproblem eller licensfrågor. Du kan däremot inte kontrollera behörighet på enhetsnivå med lösenord, installera program och uppdateringar eller distribuera e-böcker eller annat innehåll på enheterna. Då måste du använda en MDM-programprofil (SMDM) eller en agent på själva enheten.

Med Aerohives klientklassificeringsfunktion får administratörerna flera lager med nätverksbaserad regelefterlevnad för mobila enheter, som börjar med den första användarautentiseringen. Det är viktigt eftersom det innebär att användarens identitet är den första variabeln som används när behörigheten definieras baserat på uppgifter som enhetstyp, plats och domänmedlemskap. Det innebär till exempel att du kan skilja på privata enheter, t.ex. om en iPad-platta tillhör en person i ledningsgruppen eller försäljningsteamet. Du kan införa olika regler för användarna som inte bara baseras på deras enhet utan även på deras identitet istället för att ha en enda regel som gäller alla anslutna iPad-plattor.



När den nya profilen har tilldelats med utgång från identitet, förändras behörigheten till nätverket beroende på vilka regler för brandvägg, tunnel och schema som har konfigurerats för den nya profilen. En av de vanligaste funktionerna som garanterar uppdelning av enskilda enheter på nätverket är en inbyggd "stateful firewall" i alla Aerohive-enheter. Även om alla användare och enheter är anslutna till samma VLAN kan administratören ändå införa regler för användare och nätverksresurser. Det gör att regelefterlevnaden kan vara exakt och tillämpas när trafiken först kommer in i nätverket, istället för att den begränsas när den har nått långt in. Administratören kan till exempel vilja hålla den anställdas privata enhet på samma nätverk som företagsdistribuerade betrodda klienter utan att låta den privata enheten komma åt känsliga företagsresurser när den är tänkt att användas till internetåtkomst.

Ett annat vanligt sätt att dela upp trafiken är att använda tunnelfunktioner med tre lager. Funktionen används ofta för att ansluta olika virtuella LAN-nätverk i en anläggning för smidig roaming mellan undernätverk. Den kan även användas för att överföra roamingtrafiken till en särskild accesspunkt baserat på identitet och enhetstyp. Istället för att konfigurera ett gäst-VLAN som stöder privata enheter kan administratören definiera en regel där alla privata enheter som identifieras automatiskt skickas till en accesspunkt i en skyddszon (DMZ). Det förenklar nätverkskonfigurationen men garanterar ändå att den privata enheten separeras helt från företagsnätverket.

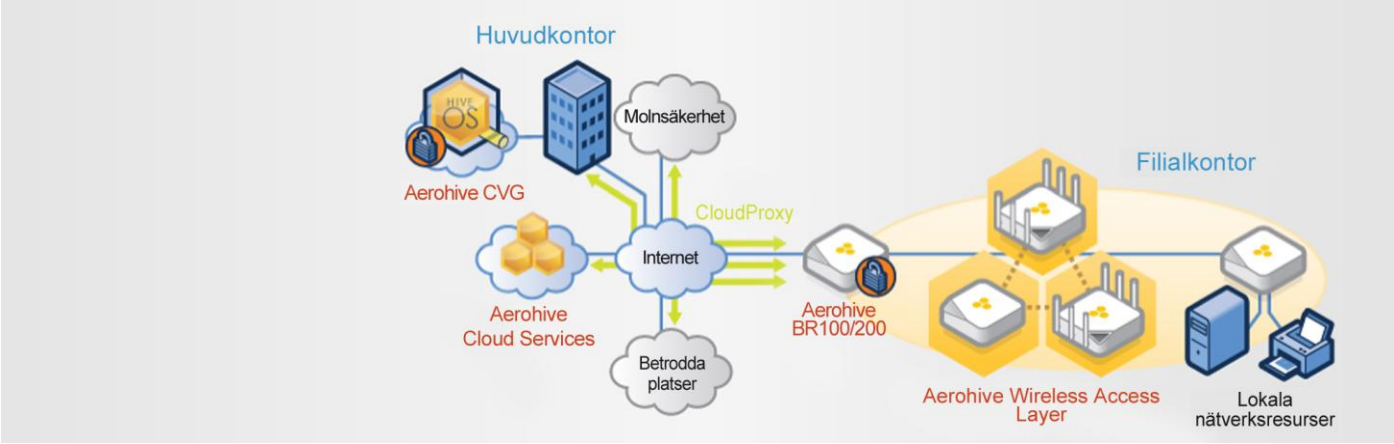
Ansluta fjärranvändare

Den sista pusselbiten i BYOD är att kontrollera att de anställda fortfarande är produktiva och ansluter till viktiga resurser, oavsett var de befinner sig – på huvudkontoret, på en filial eller hemma. När administratören har definierat nätverkets åtkomstregler, konfigurerat tillgängliga SSID och VLAN-nätverk och skapat regler för behörighet baserade på identitet och enhetstyp, ska samma regler gälla alla enheter som ansluts till företagsnätverket, oavsett var enheten och användaren befinner sig. Med Aerohive får alla anslutna användare en smidig fjärråtkomst genom IPsec VPN. Det finns två olika IPsec-alternativ som administratören kan använda för att ansluta användare, baserat på om de vill använda fullständiga fjärrnätverksfunktioner där de befinner sig eller bara utöka det befintliga företagsnätverket till filialen.

Med Aerohive Layer 2 IPsec VPN kan administratören ansluta två Aerohive-accesspunkter och smidigt utöka det befintliga nätverket så att filialen omfattas. Fjärraccesspunkten tar trafiken från filialen till accesspunkten på huvudkontoret och alla regler som administratören har konfigurerat för åtkomst till det nätverket används för de användare som ansluts från filialen. Lösningen är särskilt praktisk för enheter eller program som kräver sändningsstöd på samma virtuella LAN för att fungera på rätt sätt. Det

kan däremot uppstå problem med att skala om många enheter på flera olika filialer försöker använda samma Layer 2-nätverk samtidigt.

Ett annat alternativ för fjärranslutning av användare och enheter är Aerohives Branch on Demand-lösning. Aerohives filialroutrar ger stöd för IPsec VPN med tre fullständiga lager samt gränsbaserade nätverk med kabelanslutet och trådlöst stöd för anställda samt åtkomst med privata enheter. Branch on Demand har utformats från botten upp för att ge samma anslutningsupplevelse som på huvudkontoret, oavsett var användaren befinner sig (i butiker, hälsoinrättningar, filialer eller hemma).



Förutom att utvidga företagsnätverket till fjärranslutna användare och enheter ger Aerohives filialroutrar stöd för fullständig regelefterlevnad i Enterprise Class för privata enheter, med klientklassificering och fullständig "stateful firewall".

VAD HÄNDER SEDAN? Garanterad produktivitet för anslutna användare

När administratören har definierat åtkomst- och autentiseringsbehörighet och är ganska säker på att de många olika enheterna som ansluts till företagsnätverket autentiseras och säkras på rätt sätt, kommer nästa stora utmaning.

Det är ingen nyhet längre att kunna ansluta enheter till nätverket. Som du ser ovan finns det många olika alternativ för att kontrollera att enheterna ansluts till nätverket och integreras eller delas upp i enlighet med de säkerhetsregler som administratören anger. Alla nätverksleverantörer måste ha en eller flera lösningar för att kunna ansluta privata enheter till nätverket på ett enkelt och säkert sätt. Det ingår i processen att planera och bygga upp ett nätverk som klarar de många olika enheter som ska anslutas. Det måste tas med i beräkningen när potentiella nätverkslösningar utvärderas.

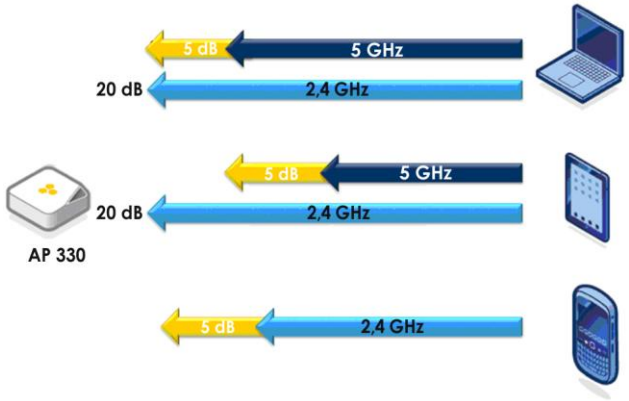
Det som verkligen tar tid för it-avdelningen är att kontrollera vad enheterna gör när de är anslutna till nätverket och hur nätverket påverkas. Om it-chefen har planerat att det ska finnas it-resurser för en företagsdistribuerad dator och en telefon per användare samt en eller några skrivare per byggnad och it-avdelningen helt plötsligt blir nedringd med frågor om de tre till fem enheter per person som varje användare har med sig, faller systemet nästan omedelbart. Fördelen med att använda privata enheter och att distribuera konsumentenheter (eftersom de är enklare att använda och kostar mindre) uppvägs snabbt av den ökade belastningen på de tillgängliga resurserna. Hanteringen av enheterna när de är anslutna till nätverket är det verkliga testet för stabila, skalbara och enkla nätverkslösningar för företag.

Bättre anslutningsmöjligheter

Ansluta enheterna till nätverket på ett säkert sätt är bara det första steget till en omfattande lösning för mobila enheter inom företaget. En annan viktig aspekt är att hålla dem anslutna och se till att de ger en smidig och produktiv arbetsupplevelse när de är anslutna till nätverket. Eftersom många av dessa enheter är särskilt utformade för konsumentanvändning på hemmanätverk har fokus oftast lagts på längre batteritider och användarupplevelse, och inte på de bästa Wi-Fi-funktionerna för överföring och mottagning. Aerohives accesspunkter och routrar är särskilt utformade för en bättre Wi-Fi-upplevelse med konsumentmottagare i mobila enheter.

En av de mest missförstådda aspekterna när det gäller att bygga Wi-Fi-nätverk är att lägga fokus enbart på att accesspunkten skickar starkare och högre signaler. Även om myndigheterna inte skulle begränsa styrkan på Wi-Fi-sändare skulle det bara lösa halva problemet att öka sändningsstyrkan. Klientenheten skulle höra accesspunktens kraftiga sändning men skulle inte kunna svara med en signal på samma nivå, vilket skulle innebära att accesspunkten inte skulle kunna ta emot klientens svarssignal. Det är lite som att skrika i en megafon till någon som står på andra sidan en fotbollsplan. Även om personen i fråga kan höra dig genom megafonen så hjälper det inte honom eller henne att skrika tillbaka på en nivå som du kan höra.

Moderna accesspunkter och routrar måste ha förbättrade Wi-Fi-funktioner för svaga sändningssignaler från konsumentenheter. Aerohive har en särskilt utformad antenn på accesspunkterna som ger bättre mottagning. Det betyder att Aerohives accesspunkter kan ta emot signaler från enheter med låg signalstyrka, som smartphones och surfplattor. Bättre mottagning – upp till 5 dBM per band – gör att Aerohive-enheterna kan ta emot radiosändningar med bättre kvalitet och färre fel, vilket ökar den totala överföringshastigheten och minskar andelen fel och signaler omsändningar.



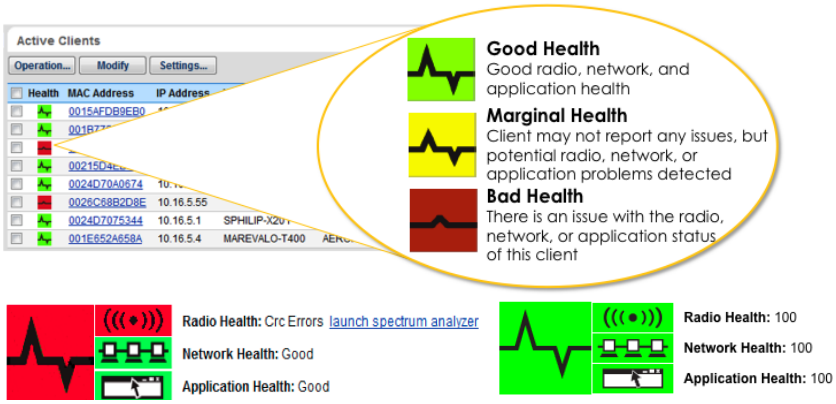
Bättre mottagning ger även fördelen att 5 Ghz-kapaciteten blir större och mer tillgänglig för klienter med stöd för 5 Ghz-bandet, vilket skapar mer utrymme på det överanvända 2,4 Ghz-spektrumet och gör att man kan använda båda spektrumen för radiokommunikation med högre hastigheter. Mer intelligenta accesspunkter i kombination med molnhanterade Cooperative Control-program ger en bättre Wi-Fi-upplevelse på alla enhetstyper, oavsett om de är konsumentfokuserade eller inte.

Effektiv BYOD-hantering

En annan vanlig utmaning för administratörer när de extra enheterna har kopplats till nätverket är frågan hur de ska hanteras och övervakas. Om enheten har svårt att komma åt resurserna får it-administratören ofta ett telefonsamtal från en användare som klagar på nätverket – för det skulle ju inte kunna tänkas vara enhetens fel, eller hur? Aerohive har flera inbyggda funktioner i accesspunkterna och routrarna som gör det enklare att hantera, övervaka och lösa problem som uppstår i samband med de många nya enheterna.

Det första steget när det gäller att identifiera problemet med en ansluten klient är att kunna fastställa om det faktiskt föreligger ett problem. Även om många it-tekniker är experter på nätverk så är de förmodligen inte experter på radiosignaler. Språket som används för omsändningar, CRC-fel och

radiosignaler kan se ut som rena grekiskan för en vanlig it-administratör. Funktionen Aerohive Client Health har tagits fram för att du inte ska behöva gissa dig fram till lösningen när du övervakar anslutna klienter. Den fastställer bästa möjliga sändningshastighet för enskilda klienter och spårar sedan statistik och potentiella problem för klienten innan den visar en enkel grön, gul eller röd ikon som representerar klientens hälsotillstånd. Funktionen kan användas till både kabelanslutna och trådlösa klienter och inkluderar även information om huruvida klientens radiohälsa eller kabelanslutning är tillräcklig, men att klienten inte kan hämta en nätverksadress via DHCP eller uppfylla det SLA som har definierats för just den användaren. Allt detta utgör ett mycket enkelt och transparent sätt att spåra klienterna – även privata enheter.



Bara förmågan att kunna se vad klienterna håller på med är användbart, men eftersom det som verkligen tar it-avdelningens kraft är att hantera de problem som kan uppstå med klienter i nätverket har Aerohives produkter även integrerade automatiska åtgärds- och mitigeringsfunktioner. Det gör att administratören kan ställa in regler för anslutna klienter med separata regler för företagsdistribuerade klienter och privata enheter eller gästenheter. Om klienthälsan faller under en viss nivå kan Aerohive-enheterna automatiskt ge den utsatta klienten större resurser. Bland funktionerna märks bandstyrning av klienten till andra radiosignaler som stöds, belastningsbalansering av klienten till en annan accesspunkt och även mer sändningstid för långsamma överföringar. På så sätt kan man undvika att signalen behöver skickas igen till den anslutna klienten om den av någon anledning inte når upp till det konfigurerade SLA-prestandamålet. Det gör att administratören kan fokusera på resten av världsproblemen istället för att oroa sig för potentiella problem med anslutna klienter.

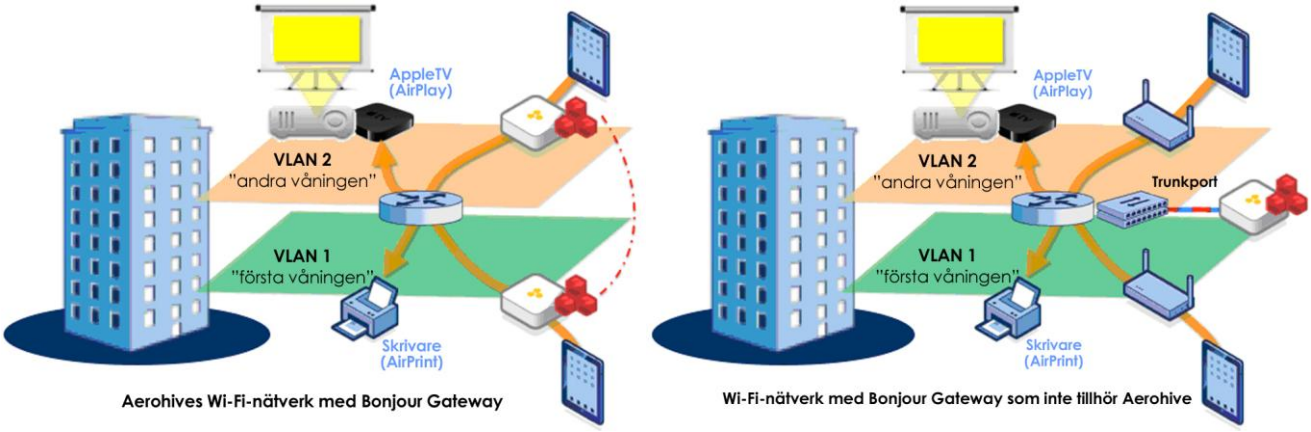
Använda BYOD för att öka produktiviteten

Låt oss för en stund föreställa oss en perfekt värld där alla anslutna klienter fungerar perfekt, nätverket fungerar som en dröm vid full prestanda och alla användare är nöjda och glada med sina möjligheter att ansluta valfri enhet till nätverket och få rätt behörighet definierad av administratören. Även i det här drömscenariot kommer användarna att vilja använda sina privata enheter, och särskilt sina företagsdistribuerade konsumentenheter, för att ansluta och använda nätverkets resurser och tjänster. Utskrifter och projektbilder är två vanliga behov som genast framhålls. Då krävs en tjänsteinriktad nätverkslösning för att BYOD ska fungera, där nätverket hjälper klienten att hitta rätt resurs utan att involvera it-avdelningen.

Om vi tittar på BYOD i allmänhet är en av de statistiska aspekterna som genast kommer upp till ytan att 72 procent av de enheter som användarna tar med sig till kontoret och vill ansluta till företagsnätverket är Apple-produkter.[4] Apple-produkter, och särskilt då iOS, använder sig av Bonjours konfigurationsfria nätverksfunktioner för att hitta tillgängliga resurser i nätverket, t.ex. skrivare eller Apple TV-enheter med projektorer. Bonjour är ett protokoll som använder sig av DNS (mDNS). Mer information om hur

[4] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals" 2011

protokollet fungerar finns i lösningssummeringen för Bonjour Gateway.[5] Ett av problemen med mDNS är att det begränsas till en enda sändningsdomän (virtuellt LAN). Om en administratör har definierat BYOD-regler som separerar klientenheter från företagsnätverket med VLAN-nätverk blir detta genast ett hinder när nätverket ska användas produktivt. Aerohive har utvecklat Bonjour Gateway så att användarna på alla VLAN kan se och använda Bonjour-stödda resurser i nätverket, oavsett var resurserna finns. Bonjour Gateway kan konfigureras så att alla tjänster släpps igenom eller begränsas så att resurserna identifieras och används beroende på identitet, plats och enhetstyp med hjälp av den inbyggda filterfunktionen.



Aerohives framstående position inom tjänstemedvetna nätverksfunktioner medför att alla enheter är produktiva i nätverket. Dessutom kan administratörerna använda inbyggda DHCP-proxyenheter och RADIUS-funktioner så att privata enheter och företagsdistribuerade enheter kan använda nätverksresurserna inom hela koncernen.

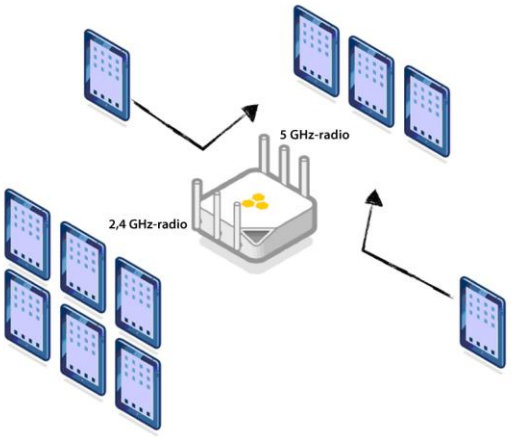
Kontrollera att nätverket klarar av mängden av privata enheter

Nu när enheterna är anslutna till nätverket och används produktivt blir det regelbundna underhållet av nätverket den huvudsakliga frågan. Många konsumentenheter som används för BYOD, och särskilt då mobiltelefoner, har endast stöd för 2,4 GHz-Wi-Fi-spektrumet. Det kan skapa stora problem i ett nätverk som har utformats för att ge stöd till färre klienter eller som redan körs med hög kapacitet. Aerohive har tagit fram flera olika funktioner som kan hjälpa till med högdensitetsanvändningen och problemlösningsfrågor som kan uppstå i miljöer där många olika enheter konkurrerar om sändningstiden.

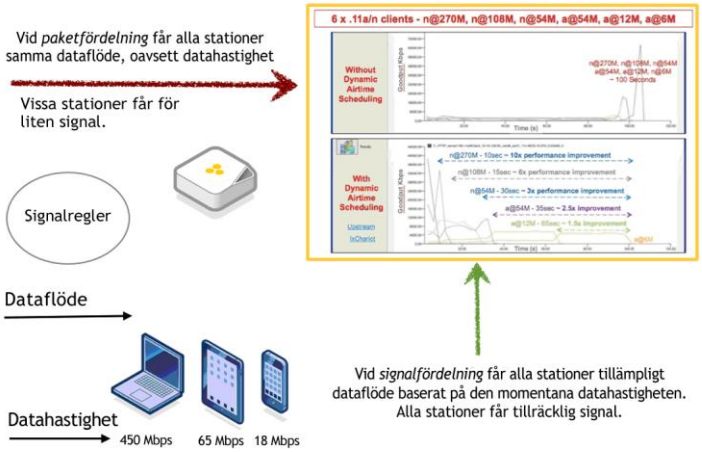
Det är tydligt från nyheterna om 802.11ac att 2,4 GHz-radiospektrumet officiellt har uppnått sin maximala kapacitet. 2,4 GHz, som begränsas av kanalkapaciteten och den allmänna överanvändningen av både oräkneliga Wi-Fi-enheter och enheter som inte använder 802.11, kommer inte att följa med 5 GHz till gigabit-Wi-Fi. Men eftersom många enheter på marknaden fortfarande bara har stöd för det här bandet är det viktigt att Wi-Fi-leverantörer ger tillräckliga funktioner för att klara den allt mer ökande belastningen på det kämpande spektrumet. Aerohive har integrerat många högdensitetsfunktioner i HiveOS, däribland en möjlighet att styra klienter med stöd för 5 GHz bort från det överbelastade 2,4 GHz-spektrumet. En viktig detalj vad gäller Aerohive är att i de sällsynta fall när 2,4 presterar bättre än 5 GHz av någon anledning (störningar, överbelastning etc.) så är Aerohive-produkten smart nog att styra klienterna till den radiosignal som är minst belastad. HiveOS kan på ett effektivt sätt balansera klientenheterna på flera accesspunkter i samma "hive" eller grupp med Cooperative Control-accesspunkter. Även om alla dina användare ansluter sina privata enheter till nätverket och sätter sig i samma samlingssal kan HiveOS enkelt och effektivt balansera klienterna över

[5] http://www.aerohive.com/pdfs/Aerohive-Solution_Brief-Bonjour_Gateway.pdf

de tillgängliga accesspunkterna och garantera att ingen accesspunkt är överbelastad med anslutna klienter.



Ett annat problem som man ofta stöter på där det finns många privata enheter är att administratören inte riktigt kan införa rättvisa regler som tillåter enheterna på nätverket och samtidigt begränsar vilka typer av enheter som användarna ansluter. Det skulle verkligen inte vara rättvist om det bara var de som hade råd att ta med sig en ny iPad med stöd för 802.11n med hög hastighet som fick ansluta sina enheter. Därför måste administratören och nätverket acceptera att vissa användare fortfarande kommer med enheter som använder 802.11b. Det betyder att nätverket måste kunna kompensera för de långsamma och mindre effektiva gamla enheterna. Aerohives Dynamic Airtime Scheduling identifierar automatiskt den maximala hastigheten som varje enhet har stöd för baserat på klienttyp och avstånd från accesspunkten och balanserar sedan sändningstiden mellan klienterna. Det är inte längre så att en enda långsam klient kan stoppa upp hela det trådlösa nätverket. HiveOS övervakar kontinuerligt den maximala potentialen för alla anslutna klienter och garanterar att nätverket utnyttjas med bästa möjliga prestanda och hastighet. Klienter som faller under ett definierat SLA kan automatiskt få mer sändningstid av HiveOS så att klientens prestanda höjs och uppfyller kraven.



Höja ribban

Alla dessa funktioner i kombination innebär att Aerohive verkligen har förändrat förutsättningarna för företagsnätverk. Nu behöver man inte längre designa ett nätverk endast för företagsdistribuerade enheter. Aerohive har gjort det enkelt att inte bara ansluta konsumentklienter och privata enheter utan har även förändrat hur administratörerna hanterar och användarna använder nätverken som enheterna är anslutna till. Allt eftersom fler och fler enheter läggs till i nätverket är det viktigt att nätverkslösningen kan skala på ett effektivt och säkert sätt och ge alla enheter åtkomst i Enterprise Class, även konsumentenheterna. Detta blir mer och mer tydligt allt eftersom mobila enheter får högre

hastigheter och blir mer effektiva och användarnas förväntningar på vad som ska finnas tillgängligt för dem bara ökar, oavsett var de är eller vilken tid på dygnet det är.

Aerohives Cooperative Control-arkitektur gör det möjligt för administratören att bygga ett nätverk utformat för både dagens och morgondagens behov, vilket gör din investering framtidssäker och redo för nästa våg av mobila användare och enheter. Vår kundanpassade och tjänstemedvetna nätverksinfrastruktur ger hög prestanda inom nätverket, oavsett om du ansluter en tio år gammal skanner eller en toppmodern gigabit-Wi-Fi-klient med 802.11ac. Aerohives molnaktiverade nätverk med distribuerad intelligens ger inbyggd nätverksbaserad MDM, involverar iEverything-explosionen av BYOD och förenklar de komplexa nätverksproblem som företag står inför när de önskar hantera mobila höghastighetsenheter.

Läs mer om Aerohives Cooperative Control-arkitektur och marknadsledande funktioner för produktiv Wi-Fi-användning på www.aerohive.com. Där finns även mer information om BYOD och konsumentanpassning av it och hur de påverkar företagsnätverket. Anmäl dig för en demo och bygg en egen plan över hur du kan designa om ditt nätverk så att det klarar nästa steg i den mobila invasionen.

Om Aerohive

Aerohive Networks reducerar kostnaderna och komplexiteten i dagens nätverk med hjälp av molnaktiverade, distribuerade Wi-Fi- och routinglösningar för organisationer och medelstora företag, inklusive filialer och fältanvändare. Aerohives prisbelönta Cooperative Control-arkitektur för Wi-Fi, publika och privata molnaktiverade nätverkshantering samt routing- och VPN-lösningar eliminerar behovet av kostsamma kontrollers och felpunkter. Det ger kunderna verksamhetskritisk tillförlitlighet med granulär säkerhets- och regelefterlevnad samt möjligheten att börja i liten skala och sedan utveckla systemet utan några begränsningar. Aerohive grundades 2006 och har sitt huvudkontor i Sunnyvale i Kalifornien. Företagets investerare utgörs av Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital och New Enterprise Associates, Inc. (NEA).

Huvudkontor
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089, USA
Tfn: +1 408 510 6100
Avgiftsfritt nummer: +1 866 918 9918
Fax: +1 408 510 6199
info@aerohive.com
www.aerohive.com

Internationellt huvudkontor
Aerohive Networks Europe LTD
The Court Yard
16–18 West Street
Farnham, Surrey, GU9 7DR, Storbritannien
+ 44 (0) 1252 736590
Fax: + 44 (0) 1252 711901

WP1206011