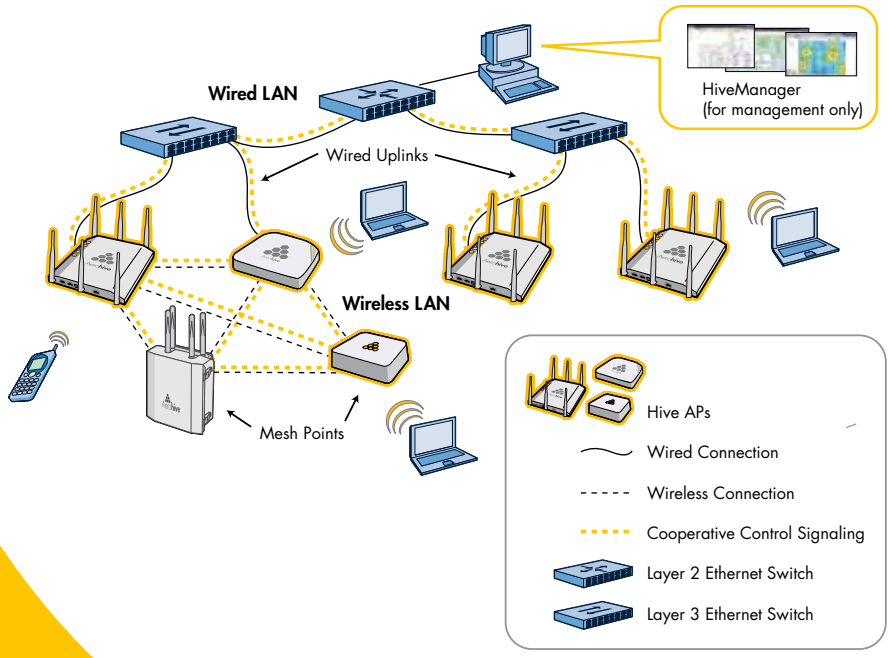
Arquitectura WLAN de control cooperativo - Aerohive Networks

La evolución de las redes inalámbricas ha ido adquiriendo gran importancia en muchos sectores como respuesta a una demanda de acceso a aplicaciones críticas en tiempo real. Además, la continua migración desde puntos de acceso autónomos y la llegada de 802.11n requieren de nuevas arquitecturas WLAN más potentes, seguras, sencillas de desplegar y ampliar que las generaciones anteriores de redes inalámbricas.

La primera oleada de WLANs eran puntos de acceso autónomos y relativamente fáciles de desplegar y que cumplían con la demanda de entonces. Hoy en día la demanda se dirije hacía una movilidad, manejabilidad y seguridad avanzada para redes críticas. Después, surgirían las actuales arquitecturas centrales basadas en controlador, que solucionaban estos problemas y que añadían además, gestión centralizada y roaming entre dispositivos proporcionando una gestión coordinada y una política de seguridad a estas redes. Pero desgraciadamente, este tipo de arquitecturas también supuso nuevos problemas como redes superpuestas opacas, cuellos de botella, puntos únicos de fallo, latencia aumentada y costes considerablemente más elevados para las redes empresariales.

Aerohive Networks representa un gran paso hacia una arquitectura WLAN de control cooperativo. Nace de 11n y ofrece una solución sumamente rentable para las empresas de hoy en día, que requieren alta disponibilidad y seguridad. Con una innovadora propuesta basada en Puntos de Accesos inteligentes, Aerohive aporta una mayor facilidad de despliegue, escalabilidad, rentabilidad y ahorro de costes que las infraestructuras basadas en controlador, pero con los mismos beneficios de éstas en lo relativo a seguridad.



Aerohive NETWORKS

Funcionalidades

La arquitectura de control cooperativo de Aerohive Networks combina puntos de acceso de clase empresarial con un conjunto de protocolos y funciones cooperativas para proporcionar todos los beneficios de una solución WLAN basada en controlador, pero sin requerir un controlador o una red superpuesta. Esta funcionalidad de Control Cooperativo permite organizar múltiples APs cooperativos en grupos llamados "Hives", los cuales comparten datos de control entre APs para habilitar funciones como roaming rápido y seguro de capa 2 y capa 3, gestión RF coordinada, seguridad, QoS y redes malladas.

Para crear una arquitectura de control cooperativo, Aerohive ha desarrollado HiveAPs de nueva generación con funcionalidades de alta gama, que ofrecen:

- Radios duales para permitir el uso simultáneo de IEEE 802.11b/g en adicción a IEEE 802.11a para acceso inalámbrico y conectividad de red mallada inalámbrica;
- Un conjunto de protocolos de control cooperativo para proporcionar enrutamiento dinámico basado en la MAC, selección automática de canales de radio y un roaming rápido.
- Un appliance de gestión centralizada para tareas simplificadas de configuración, monitorización y troubleshooting;
- Seguridad robusta con IEEE 802.1X, lo último en los estándares IEEE 802.11i, reglas de firewall y prevención de DoS (denegación de servicio) de capas 2 a 4.

Ventajas competitivas

Auto-descubrimiento y auto-organización de Puntos de Accesos

El Control Cooperativo simplifica el despliegue de un conjunto de puntos de acceso que pueden autodescubrirse por sincronización proactiva tanto si están conectados mediante red cableada o inalámbricamente. Una vez se han establecido las relaciones contiguas entre HiveAPs en un Hive, se ejecutarán los protocolos de Control Cooperativo para proporcionar un roaming, control RF automático y capacidad de recuperación rápidos y seguros.

Balanceo de carga de túneles en entornos de roaming de capa 3 a gran escala

La característica de roaming rápido de Aerohive proporciona una escabilidad sin precedentes usando el balanceo de carga de túneles, lo cual aprovecha el procesamiento de potencia distribuido de la red inalámbrica para escalar y soportar miles de túneles de roaming de capa 3 y múltiples gigabits de caudal a través de subredes.

Control RF cooperativo

Para eliminar interferencias de canales de radio y para poder reaccionar a cambios en el entorno RF, los HiveAPs usan Aerohive Channel Selection Protocol (ACSP) para cooperar entre sí y seleccionar automáticamente los mejores canales de radio para un rendimiento óptimo de la red inalámbrica.

Balanceo de carga de estación

En caso de sobrecarga de un HiveAP basado en la carga total del sistema, la carga de tráfico de voz de estaciones asociadas, el número total de estaciones asociadas y la calidad de la señal de estaciones asociadas, un HiveAP puede tomar decisiones para descargar estaciones desde un HiveAP que se pueden gestionar mejor por otro y hacer funciones de control de admisión a estaciones para impedir sobreutilización.

Aplicación de política en el acceso

Usando la aplicación de política en el acceso, los HiveAPs pueden forzar una seguridad basada en identidad potente y flexible, control de acceso y políticas QoS en el acceso a la red lo cual permite la denegación de servicio y motores firewall para validar tráfico en el punto de entrada antes de que se transmita a través del HiveAP.

Perfíles de usuario y política basada en identidad

La solución WLAN de Aerohive define diferentes conjuntos de políticas de acceso para diferentes clases de usuarios a través de la creación de perfiles de usuarios. Cada perfíl de usuario define una VLAN, política QoS, política firewall de MAC, política firewall de IP y política de roaming de capa 3 que se asigna a usuarios cuando conectan al WLAN.

AMRP
(Aerohive Mobility Routing Protocol)

Los HiveAPs tienen la capacidad de descubrirse unos a otros y si se encuentran vecinos con las mismas credenciales de movilidad, pueden establecer conexiones seguras entre sí por enlaces ascendentes cableados con AES, y enlaces ascendentes inalámbricos usando WPA con AES-CCMP. De este modo, los HiveAPs cooperan entre sí para determinar la mejor ruta en la red inalámbrica y con capacidad de reenviar tráfico localmente usando la mejor ruta.

ACSP
(Aerohive Channel Selection Protocol)

Los HiveAPs analizan las ondas y cooperan juntos para determinar la mejor configuración de canales de radio para el acceso inalámbrico en la red mallada inalámbrica. ACSP evita la interferencia del mismo canal de radio o contiguos para proporcionar un rendimiento WLAN optimizado. Si un dispositivo que causa interferencias aparece dentro del canal de radio actualmente operativo, el ACSP tiene la capacidad de provocar el cambio a un nuevo canal. Además, los administradores tienen la opción de permitir los cambios de canal de radio sólo si no hay estaciones asociadas, evitando que los clientes se desconecten debido a esos cambios.

DNXP
(Dynamic Network Extension Protocol)

Permite la extensión de redes de capa 2 a través de dominios enrutados de capa 3, así como roaming de capa 3 transparente y el tunelamiento dinámico a redes remotas basadas en la identidad de un cliente o el identificador de conjunto de servicios (SSID). Dentro de una subred, el DNXP puede fijar manualmente o elegir automáticamente los HiveAPs responsables de facilitar la creación dinámica de rutas tuneladas entre HiveAPs dentro de subredes diferentes.

EXCLUSIVE NETWORKS

Aplicación de política QoS en el acceso

Aerohive ha desarrollado motores QoS avanzados dentro de cada HiveAP para asegurar un rendimiento óptimo para tráficos de prioridad alta y baja. Esto proporciona mayor escabilidad sin cuellos de botella.

Aplicación de política de seguridad en el acceso

Con la arquitectura de LAN inalámbrica de Control Cooperativo, la política de seguridad es gestionada de forma centralizada utilizando el HiveManager, pero esta es aplicada en el acceso inalámbrico en cada HiveAP. Esto permite a los HiveAPs aplicar políticas avanzadas de seguridad localmente en el punto de entrada pudiendo utilizarse los sistemas de seguridad actuales puestos en la red cableada -firewalls, gateways de antivirus, IDPS, y dispositivos de control de acceso a la red (NAC)- para aplicar políticas en el tráfico inalámbrico también.

Portal web cautivo integrado

Otra forma de proporcionar la aplicación de políticas en el acceso es con la utilización de un portal web cautivo integrado en cada HiveAP. Cuando un usuario se asocia con un SSID con el portal web cautivo activado, y abren su navegador, son redirigidos a una página web de registro.

Túneles basados en identidad

Se puede usar la misma tecnología que da a los HiveAPs la capacidad de ejecutar roaming de capa 3 para tunelar los clientes inalámbricos a un HiveAP en una red diferente basada en su identidad. Esta se puede usar en entornos donde los invitados se envían al DMZ o donde el switch de acceso no admite VLANs.

El reenvío por la mejor ruta

La mejor ruta es la ruta más corta y la latencia más baja a un recurso de red. Con el reenvío de la mejor ruta de Aerohive, cada HiveAP coopera con los HiveAPs contiguos para encontrar rutas óptimas entre ellos, clientes y la red cableada.

Red mallada inalámbrica

Por toda la red mallada inalámbrica, se usan los protocolos de Control Cooperativo de Aerohive para proporcionar el reenvío por la mejor ruta, roaming rápido y seguro, selección óptima de canales de radio y alimentación de energía para conexiones inalámbricas y alta disponibilidad con enrutamiento dinámico y reenrutamiento stateful del tráfico en caso de fallo eventual.

Seguridad en el HiveAP

Utilizando la arquitectura WLAN de Control Cooperativo con el reenvío por la mejor ruta, autenticación, encriptación, mitigación de DoS y control de acceso firewall, se aplica la seguridad en el HiveAP antes de que se reenvíe el tráfico dentro de la red.

Escalabilidad

Cada HiveAP toma sus propias decisiones de reenvío y usa el reenvío por la mejor ruta para transmitir datos. Sin un dispositivo de reenvío de tráfico central que puede convertirse en un cuello de botella, los HiveAPs pueden aprovechar el rendimiento y la capacidad de la infraestructura de la red cableada, dando un rendimiento completo sin bloqueos.

Alta disponibilidad

Las características de alta disponibilidad de Aerohive vienen por defecto con los HiveAPs y proporcionan muchos niveles de capacidad de recuperación y redundancia.

Ningún punto único de fallo

La arquitectura WLAN de Aerohive Networks no tiene un punto único de fallo. Si un único HiveAP falla, las estaciones cambian automáticamente a HiveAPs contiguos igual que si estuviesen haciendo roaming, sin perder la autenticación, seguridad, parámetros de QoS o estado de sesión, y sin interrumpir conexiones críticas de datos o voz.

HiveAPs con el servidor RADIUS integrado

Con un servidor RADIUS integrado en los HiveAPs, los administradores tienen la posibilidad de implementar la red inalámbrica segura con la autenticación IEEE 802.1X EAP para sus clientes inalámbricos, sin tener que configurar o modificar servidores RADIUS corporativos.

Cachés de credenciales AAA

Aerohive proporciona la posibilidad de guardar nombres de usuario y hashes de contraseñas en DRAM para que en el caso de fallo de la WAN, la autenticación siga funcionando.

Ventajas competitivas (continúa)

Gestión centralizada

Un sistema de gestión de la red central llamado HiveManager proporciona la configuración centralizada, la monitorización y los informes. Se puede ubicar este appliance de gestión en cualquier parte dentro de la red y no es esencial para la operación normal de la red.

Gestión de configuración simplificada

El interfaz gráfico de gestión para el HiveManager se ha diseñado para que miles de HiveAPs se puedan gestionar y monitorizar utilizando perfiles de configuración. Los perfiles de HiveAP son un mecanismo muy potente utilizado para organizar y aplicar una configuración a un gran número de HiveAPs. Basado en la ubicación o en un tipo de despliegue lógico, los perfiles de HiveAP asignan perfiles de configuración y definen asociaciones desde SSIDs a perfiles de usuario e identificadores de VLAN.

Cero configuración para despliegues de puntos de acceso inalámbricos

Cuando los HiveAPs se encienden y conectan a una red que utiliza DHCP o DNS, pueden aprender automáticamente la información requerida para contactar con el HiveManager. Entonces los HiveAPs usan CAPWAP para contactar con el HiveManager e identificarse así mismos. Una vez identificados, el HiveManager muestra una lista de los nuevos HiveAPs descubiertos

Monitorización, informes y resolución de problemas simplificado

Junto con una configuración y gestión de sistema operativo simplificada, el HiveManager hace sencillo monitorizar y resolver problemas de los HiveAPs en una infraestructura de red inalámbrica. Desde cualquier mapa de topología o desde una lista filtrable y ordenable de HiveAPs gestionados, los administradores pueden ver información en tiempo real como un listado de clientes inalámbricos asociados, logs, información de roaming, configuraciones y estadísticas. El HiveManager también permite ver todos los clientes activos en la WLAN, mostrando su dirección IP, dirección MAC, hostname, nombre de usuario (si utiliza 802.1X), SSIDs, tiempos de inicio de sesión, valores de fuerza de la señal, y los HiveAPs a los que están conectados los clientes. Esta información se almacena en el HiveManager y puede exportarse para la resolución de problemas avanzado.

Detección de APs no autorizados

Usando el HiveManager, los administradores pueden configurar políticas de detección de puntos de acceso no autorizados para buscar APs que no tienen un BSSID, SSID, configuración de autenticación y encriptación, y otros ajustes de configuración más finos que sean válidos. Además los HiveAPs pueden detectar si los no autorizados están en la misma subred y descubrir si están en la red corporativa o no.

Aerohive Networks provee de nuevas soluciones de arquitectura de control cooperativo wireless LAN, con toda la gestión y seguridad de las arquitecturas basadas en controlador pero sin los costes asociados de éstas, mayor rendimiento, flexibilidad de despliegue y escalables para soporte 802.11n.

www.aerohive-networks.com