

# A ARQUITETURA MOBILE FIRST DA ARUBA

# Índice

---

Introdução.....	1
Projeto.....	2
Casos de uso.....	2
Underlay.....	3
Overlay.....	3
Segmentação Dinâmica.....	3
Rede Sem Interrupções.....	4
Resumo.....	5

# Introdução

---

A arquitetura de rede da Aruba para a empresa definida por software foi projetada para ser mobile first, e fornece uma rede aberta, segura e autônoma. A velocidade, a variedade e o volume de usuários e coisas que se conectam às redes forçaram a mudar a maneira como constroem e operam as redes de próxima geração.

- **Mobile First**—Permite que usuários e coisas se conectem à rede e recebam a mesma política e permissões, independentemente de como eles se conectam, com ou sem fio, tornando-os verdadeiramente móveis. Projetado especificamente para fornecer uma experiência de rede ininterrupta para ambientes em que o mobile, a IoT e a nuvem são essenciais para a missão.
- **Aberta**—As redes são de vários fornecedores e precisam ser abertas. Isso significa não só oferecer suporte a padrões abertos, mas também fornecer suporte avançado a API para permitir uma fácil integração e automação de ponta a ponta na rede por parte do TI, da linha de negócios e até mesmo dos usuários. As organizações precisam ser capazes de inovar em seu ritmo e não serem bloqueadas e limitadas pela arquitetura de um único fornecedor.
- **Segura**—A segurança em todas as camadas da rede é crítica. A Aruba protege a infraestrutura com e sem fio com código assinado, inicialização segura e proteção de hardware criptográfica. Os dados do usuário são protegidos com uma forte política de criptografia e por nível de usuário, garantindo acesso apropriado e protegendo dispositivos contra ameaças. A segurança orientada pelo Analytics, o gerenciamento de políticas líder de mercado, e um extenso ecossistema de parceiros de segurança confiáveis permitem que a equipe de TI projete e opere sua rede.
- **Autônoma**—O aprendizado de máquina usa grandes quantidades de dados analíticos para entender o estado operacional e de segurança da rede. Os sistemas automatizados otimizam o desempenho e alertam aos administradores sobre alterações ou destacam possíveis mudanças que exigem aceitação por meio de operações de rede gerenciadas no local e na nuvem.

As redes tradicionais tornaram-se uma confusão de VLANs e ACLs porque as organizações reforçaram a política e a segurança numa infraestrutura que nunca foi desenvolvida para lidar com políticas baseadas em aplicações. As portas de um switch têm configurações estáticas e as interfaces de VLAN têm centenas, às vezes milhares de ACLs — levando a projetos de rede que são frágeis e que a equipe de TI tem receio de mexer.

# Projeto

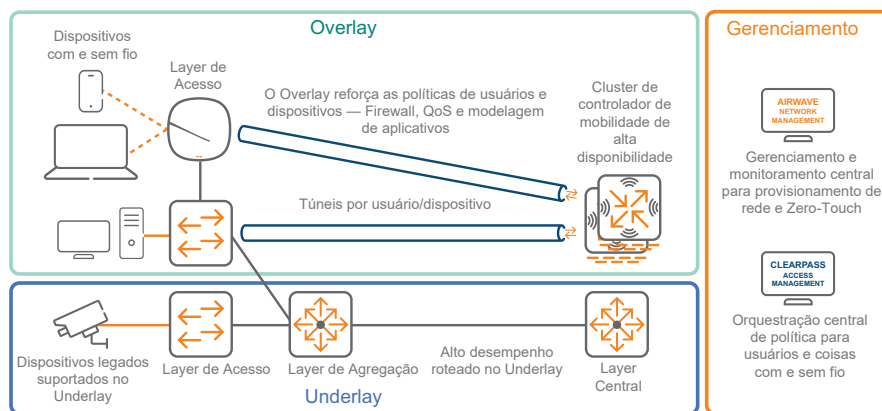
Não há uma rede no futuro; há milhares, e a Aruba está fornecendo infraestrutura com um modelo para suportar a diversidade e a complexidade necessárias nas redes definidas por software de próxima geração. Na empresa definida por software, a equipe de TI executa a infraestrutura e a rede subjacente, e dá aos usuários e à linha de negócios a capacidade de auto-provisionar redes de sobreposição.

## CASOS DE USO

- **Acesso de convidado temporário aos recursos de rede** — Os usuários podem criar contas de convidado temporário e dar permissão para acessar recursos de rede, como sistemas de vídeo na sala de conferência, impressoras e Internet, por meio de uma sobreposição segura e efêmera.
- **As instalações precisam permitir o acesso do fornecedor à construção de sistemas de IoT** — O gerente do edifício pode criar uma sobreposição de IoT segura para os sistemas de controle da construção e fornecer o serviço VPN ao fornecedor, para que ele possa acessar e monitorar o equipamento.
- **Os usuários têm dispositivos e desejam sua própria rede pessoal** — Os usuários com vários dispositivos com fio e sem fio precisam acessá-los com segurança e permitir que se comuniquem entre si, independentemente de como eles se conectam à rede da organização.

Entregar a rede como um serviço aos usuários é o núcleo da empresa definida por software. O BYOD e sua normalização mostraram que a equipe de TI precisa ser capaz de oferecer suporte a uma ampla gama de dispositivos de usuários, e a avalanche de dispositivos IoT significa que a escala do que precisa ser suportado está além do que um grupo de TI em frente a um sistema de gerenciamento pode aguentar. Ferramentas que permitem à equipe de TI delegar a criação de serviços aos usuários, com base em privilégios definidos, são necessárias para habilitar à empresa e evitar toda uma nova onda de TI de sombra.

Figura 1 Primeira arquitetura do Aruba Mobile



## UNDERLAY

As redes corporativas precisam suportar os endpoints atuais, incluindo muitos sistemas legados, enquanto fazem a transição para um modelo definido por software. Projetos que exigem uma reformulação completa da rede, incluindo hardware e stack de protocolo de rede, podem causar sérios problemas de interrupção e compatibilidade de risco, especialmente com sistemas legados. O Mobile First mantém a rede roteada existente, usando um protocolo de gateway interior padrão (IGP) — como o OSPF — como um underlay, permitindo que a equipe de TI continue com a execução e operação do hardware existente quando a nova rede for implantada. Os dispositivos legados podem continuar a operar no underlay e os aprimoramentos na política permitem segurança adicional e controle de rede além do que é comumente implantado em redes tradicionais.

## OVERLAY

O overlay permite que as organizações encapsulem com segurança o tráfego da Camada 2 ou da Camada 3 sobre a rede existente. A Aruba vem fornecendo redes sem fio com um modelo de overlay desde o início, permitindo que a TI forneça serviços que não seriam seguros ou estáveis em redes de vários fornecedores. A Aruba está ampliando essa funcionalidade para redes com fio, permitindo que o switch da camada de acesso atue como um “ponto de acesso com fio”. O tráfego de rede de usuários e dispositivos com fio e sem fio é tunelado para clusters centralizados de controladores de mobilidade. Todas as políticas de nível de usuário e dispositivo podem ser aplicadas na sobreposição usando o firewall do controlador de mobilidade, QoS e modelagem de tráfego, e o contexto do usuário é facilmente compartilhado com outros domínios. As estruturas de endereços VLAN e IP existentes podem ser mantidas, mas como a política é aplicada nos níveis de usuário e grupo, a VLAN e o endereço IP não estão vinculados à política.

## SEGMENTAÇÃO DINÂMICA

A Arquitetura Mobile First da Aruba não depende de configurações de porta estática, VLANs ou listas de acesso em access points — nem de switches de acesso na rede — para aplicar políticas a usuários e dispositivos.

- **Nó de Túnel** — Permite que um switch de acesso atue como um “ponto de acesso com fio”. Os usuários que se conectam ao switch podem passar por um túnel até o controlador de mobilidade, para fornecer a mesma política e experiência do usuário que quando estão conectados à rede sem fio. Para alta disponibilidade, vários túneis são criados e, se um controlador precisar ser colocado off-line para manutenção ou ocorrer uma indisponibilidade não planejada, o usuário passará facilmente para um controlador em espera.
- **Funções Transferíveis** — Se usuários ou dispositivos legados se conectarem à rede com fio e precisarem de conectividade direta com o underlay, as funções transferíveis permitirão que a configuração da porta de acesso seja carregada dinamicamente com base na postura e na política do usuário e do dispositivo.
- **Política Centralizada** — O Aruba ClearPass processa todos os usuários e dispositivos conectados à rede. Os dispositivos podem ser perfilados na conexão com a rede, ter a postura verificada e, em seguida, a política apropriada é baixada para a porta de acesso.

- **Confiança Adaptável** — Depois que os dispositivos recebem acesso à rede, seu comportamento é continuamente monitorado por ferramentas analíticas comportamentais, firewall e sistemas IPS. Se a postura de segurança do dispositivo mudar, um analista de segurança pode executar várias ações manuais ou automatizadas, como reautenticação, para verificar o usuário, colocar o dispositivo em quarentena, com acesso limitado aos recursos da rede, para facilitar a correção ou isolar totalmente o dispositivo da rede enquanto quaisquer incidentes são investigados. Se tudo estiver certo ou o dispositivo for corrigido, o analista de segurança pode restaurar rapidamente o acesso padrão.

A segmentação dinâmica da Aruba permite que as organizações conectem usuários e dispositivos a portas com fio e as encapsulem a um controlador, ou conecte-as à VLAN e sub-rede apropriadas e baixem uma política dinâmica (com configurações de segurança e QoS) à porta à qual estão conectadas. Isso amplia a funcionalidade do 802.1X tradicional com fio para fluxos de trabalho normalmente implantados somente em redes sem fio, como fácil integração de usuários de dispositivos desconhecidos (BYOD), acesso com fio ao mesmo portal cativo na rede sem fio, e suporte e remediação para dispositivos que falham na verificação de políticas ou posturas com o portal cativo.

## REDE SEM INTERRUPÇÕES

A conexão sem fio é vista como um serviço de utilidade em redes corporativas, o que significa que os usuários esperam que ela esteja sempre disponível e tenha o melhor desempenho. A arquitetura Aruba oferece vários recursos com e sem fio para oferecer suporte a redes sem fio implantadas como o serviço sem interrupções, com alta disponibilidade como parte inerente do projeto.

- **Agrupamento de Controladores** — Até 12 controladores de mobilidade da Aruba podem formar um cluster de compartilhamento de carga de alta disponibilidade, que pode ser dimensionado para centenas de Gbps de tráfego e dezenas de milhares de usuários.
- **Atualizações em Serviço** — Com o Aruba OS 8, a rede sem fio é capaz de atualizar o software em pontos de acesso e controladores, de maneira transparente, para os usuários da rede sem fio. Os usuários são guiados por APs e controladores selecionados enquanto são atualizados e, então, adicionados de volta à rede.
- **Failover Completo** — Os pontos de acesso se conectam a vários controladores em um cluster e, no caso de uma falha com o controlador primário, os pontos de acesso mudam para o secundário sem interrupção perceptível para o usuário.
- **Comutação sem Interrupções** — O Aruba OS-CX nas camadas principais e de agregação da rede oferece alta disponibilidade e atualizações sem complicações, permitindo que a TI faça a manutenção da rede sem sofrer uma interrupção.

Juntos, esses recursos permitem que uma rede Aruba forneça conexão sem fio que pode ser executada na rede de uma organização. A rede pode ser atualizada enquanto os usuários estiverem conectados, sem interrupção. E, devido à alta disponibilidade do setor, a rede pode lidar com falhas de ponto de acesso e de controlador sem que os usuários tenham seus trabalhos interrompidos.

# Resumo

---

A Arquitetura Mobile First da Aruba permite que as organizações façam uma transição harmoniosa de sua rede existente para uma empresa definida por software, permitindo novos recursos e funcionalidades, enquanto oferecem suporte a sistemas legados. Uma infraestrutura aberta de rede de vários fornecedores permite que as organizações inovem no ritmo e não fiquem presas a uma única solução de fornecedor, mas também aproveitem seus investimentos existentes. A segurança incorporada em todas as camadas da rede protege a infraestrutura, os usuários e os dispositivos contra ameaças existentes e emergentes, de fora e de dentro. O uso inteligente da análise por administradores e a automação baseada no aprendizado de máquina fornecem a garantia de rede e iniciam a mudança para uma rede de “autogestão”, na qual a TI mantém a infraestrutura, a política e os serviços de provisão de usuários dinamicamente.

© 2018 Aruba Networks, Inc. Todos os direitos reservados. Aruba Networks e o logotipo da Aruba são marcas registradas de Aruba Networks, Inc. As marcas registradas de terceiros mencionadas pertencem a seus respectivos proprietários. Para ver o contrato de software do usuário final visite [www.arubanetworks.com/assets/legal/EULA.pdf](http://www.arubanetworks.com/assets/legal/EULA.pdf)



Você pode usar o [formulário de feedback](#) para enviar sugestões e comentários sobre esta Visão geral sobre soluções.