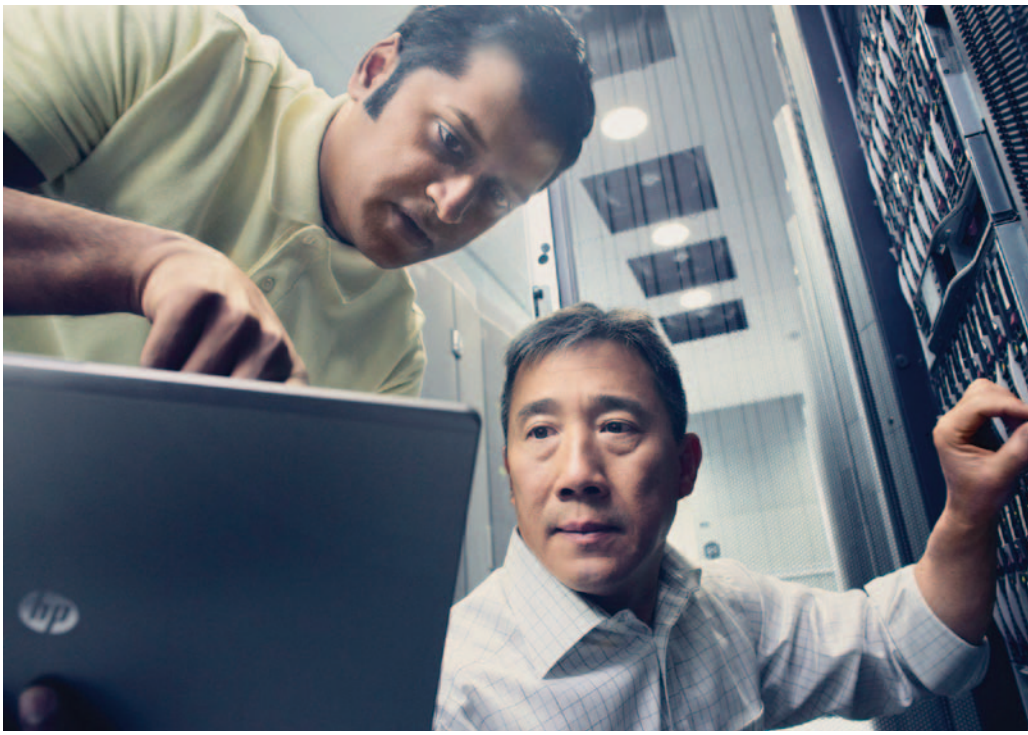
Hewlett Packard
Enterprise

비즈니스 백서

BYOD를 위한 네트워크 리-아키텍트

목차



실무 요약

개인 소유의 모바일 장치를 사용하여 회사 네트워크에 액세스하는 직원들이 점점 더 많아지고 있습니다. 많은 직원들이 직장에서 자신의 스마트폰 및 태블릿을 사용하여 생산성을 높이고 있습니다.

기업 IT 부서가 네트워크에 액세스할 수 있는 모바일 장치의 종류를 규정하던 시대는 지나갔습니다. BYOD(Bring Your Own Device) 정책은 직원 만족도 및 생산성을 개선하는 효과가 있지만, 회사 네트워크에 대한 부담을 가중시킵니다.

레거시 네트워크, 특히 캠퍼스 위치와 지사에 공통된 레거시 네트워크에는 제한적인 특성이 있으며, 유연성이 떨어지기 때문에 직원이 네트워크 사용 방식을 개인 설정하기 어렵습니다. 네트워크 설계자가 전혀 예상하지 못한 모바일 장치를 연결하는 사용자가 늘어남에 따라 보안 위험도 커지고 있습니다. 이러한 레거시 네트워크의 경우 새 장치를 연결하려면 수동으로 구성을 변경해야 하므로 새 장치를 연결하는 작업이 복잡하고 많은 노동력을 필요로 합니다. 그리고 기존의 3계층 아키텍처로 인해 최신 애플리케이션의 속도가 저하될 수 있는데 특히 무선 네트워크에서 이 현상은 더욱 심화됩니다.

회사 네트워크를 리-아키텍트하면 BYOD의 보안성과 관리 능력을 쉽게 향상할 수 있습니다. 차세대 네트워크 장비는 속도 저하를 완화하는 데 도움이 됩니다. 네트워크 업데이트로 유연성과 확장성을 개선할 수 있습니다. 또한 탁월한 네트워크 관리 애플리케이션을 통해 네트워크에 있는 장치, 해당 장치가 액세스하는 항목, 보안 유지 방식 등을 모두 단일 창 방식의 플랫폼을 통해 관리자에게 정확히 보여줄 수 있습니다.

이 백서에서는 레거시 네트워크의 한계, 특히 BYOD 지원과 관련된 제한 사항에 대해 설명합니다. 이러한 제한 사항을 이해함으로써 캠퍼스 및 지사 네트워크에 대한 BYOD 관리 정책을 성공적으로 시행하기 위한 기초를 마련할 수 있습니다.

네트워크가 걸림돌이 되고 있진 않습니까?

레거시 네트워크는 IT에서 유선 업무 네트워크에 연결된 모든 장치를 제공하는 데 사용되었습니다. 현재 사용자는 여러 장치를 사용할 가능성이 높고, 그러한 장치는 IT에서 제공하거나 승인한 것이 아닐 수도 있습니다. 또한 사용자는 비디오 스트리밍 또는 무선 네트워크를 통한 대화 내용 보관 등 장치를 복잡한 용도로 사용하기를 원합니다.

무선 네트워킹 요구가 더욱 복잡해지고 서비스가 변화함에 따라 네트워크도 그에 맞춰 대응해야 합니다. 구식 네트워크로는 그와 같은 대응이 어려울 수 있습니다. 레거시 네트워크는 다음 4가지 방식으로 BYOD를 제한합니다.

1. **경직성:** 레거시 네트워크는 IT 부서에서 사용자 및 위치 유형을 관리하도록 설계되었습니다. 직원은 네트워크 사용 방식을 개인 설정할 수 없으므로 생산성이 떨어집니다. 또한 IT 직원은 네트워크상의 기술마다 각기 다른 관리 플랫폼을 사용하고 익혀야 합니다.
2. **제한된 보안:** 레거시 네트워크는 경계가 잘 정의된 상태로 구축되었지만, 사용자가 원래의 의도대로 설계된 네트워크를 벗어난 모바일 장치에 연결하면서 보안 위험이 발생하고 있습니다.
3. **복잡성:** 무선 네트워크 구성 변경은 스크립팅 및 CLI(명령줄 인터페이스) 변경에 의존하기 때문에 시간을 들여 수작업을 해야 합니다. 무선을 통해 데이터, 비디오 및 음성을 원활하게 전송해야 하므로 네트워크 복잡성이 증폭됩니다.
4. **느린 3계층 네트워크:** 기존의 3계층 네트워크는 대부분의 직원이 데스크탑 컴퓨터를 사용하고 무선 네트워킹이 일부 경영진의 특권이던 시대에 맞게 설계된 것입니다. 2계층이 아닌 3계층을 사용할 경우 네트워크가 사용될 때마다 추가 홉(Hop)을 필요로 하기 때문에 네트워크 속도가 저하됩니다.

이러한 과제와 더불어 과제를 극복하는 방법에 대해 살펴보겠습니다.

경직성

레거시 네트워크는 고정된 구성에 맞게 설계되었습니다. 직원의 컴퓨터는 IT 부서에서 제공되며, 장비는 유선 네트워크에 연결됩니다. 각 사무실에는 네트워크 연결 지점이 있으며 설정은 변경되지 않았습니다. 직원이 네트워크나 네트워크에 연결된 장치를 필요에 맞게 조정할 수 없었으므로 IT 부서에서는 어떤 장치가 연결되어 있는지 파악할 수 있었습니다. 사용자마다 네트워크상에서 장치 하나씩을 사용한다는 개념을 바탕으로 대역폭 및 용량이 계획되었습니다. 네트워크를 구축할 때 비용을 절감하기 위해 추가 용량은 고려되지 않았습니다.

오늘날 단일 사용자는 데스크탑 컴퓨터, 노트북, 태블릿 및 스마트폰을 모두 네트워크에 동시에 연결하여 사용할 수 있습니다. 사용자는 Wi-Fi를 통해 교육 비디오를 보든, 데스크탑 컴퓨터에서 Skype 통화를 하든 상관없이 동일한 성능을 기대합니다. 작업자가 회의실 및 기타 공유 작업 공간에서 네트워크에 연결함에 따라 작업 공간 모델도 바뀌고 있습니다. 이전의 네트워크 설계는 그러한 기능을 지원하지 않습니다.

제한된 보안
레거시 네트워크에서는 보안을 엄격히 통제할 수 있었습니다. 네트워크 관리자가 허용되는 장치와 금지되는 장치를 결정했습니다. 정교한 방화벽을 통해 권한 없는 장치가 기업 데이터에 액세스하지 못하게 방지했습니다. 또한 IT 부서에서 액세스가 허용되는 모든 장치를 제공했으므로 장치가 승인된 장치인지 쉽게 알 수 있었습니다. IT 부서에서 장치를 구매하여 구축하고 원격 지원을 제공했으므로 이 모든 것이 가능했습니다.

이제는 환경이 달라졌습니다. 최상의 방화벽도 신뢰할 수 없는 장치에 대한 보호 기능을 완벽하게 제공하지 못합니다. 그러나 BYOD 보안 정책은 기본적으로 사용자가 이들 장치에 연결하는 것을 허용합니다. 보안은 더 이상 네트워크 경계 보호에만 한정되지 않으며 사용자가 네트워크에 연결하는 위치에 모두 적용되어야 합니다.

오늘날의 네트워크 관리자는 네트워크에 연결되는 장치에 대한 가시성을 필요로 합니다. 즉, 장치의 종류, 장치가 액세스하는 대상, 장치가 사용하는 대역폭 등을 파악해야 합니다. 솔루션은 새로운 서비스가 출시되는 대로 제공할 수 있을 정도로 유연성이 탁월해야 합니다. 레거시 네트워크의 한계로 인해 이러한 종류의 변경과 BYOD 보안 프로세스의 속도가 저하됩니다.

기존에는 CLI를 통해 수동으로 레거시 네트워크를 변경했습니다. 새로운 장치의 수가 증가하고 있으며, IT 부서가 네트워크에 연결되는 새로운 사용자 장치 모두를 인식할 수는 없는 환경에서 수동으로 변경하는 방법은 불가능합니다.

네트워크의 게스트 사용자는 또다른 도전 과제를 제공합니다. 사무실 방문객은 대부분 태블릿, 노트북 또는 휴대폰을 가지고 다니면서 회사 네트워크에 연결할 수 있길 바랍니다. 회사 측에서는 캠퍼스 또는 지사 시설의 방문객에게 무선 LAN 액세스를 제공하는 동시에 기업의 기밀 데이터를 안전하게 보호하기를 원합니다.

마지막으로, 직원은 보다 빠르고 안정적인 무선 액세스를 요구하고 있습니다.

복잡성
레거시 네트워크에서 네트워크의 장치 수는 상대적으로 고정적이어서 IT 관리자는 그러한 장치를 모두 인지할 수 있었습니다.

네트워크에 추가되는 기능이 증가함에 따라 관리 업무가 더 복잡해지고 있습니다. 무선 네트워크를 유선 환경에 추가할 경우 각각 두 세트의 네트워크, 관리 애플리케이션 및 보안 구현이 생기게 됩니다.

복잡성이 배가되었습니다. 알려지지 않은 장치가 네트워크에 접속되거나 해제되고 동일한 사용자가 노트북과 스마트폰으로 네트워크에 번갈아 액세스함에 따라 이러한 모든 상호 작용을 관리할 수 있는 통합 시스템을 갖추는 것이 중요합니다. CLI를 사용하여 정책을 정의하고 시행하는 것은 더 이상 현실적이지 않습니다.

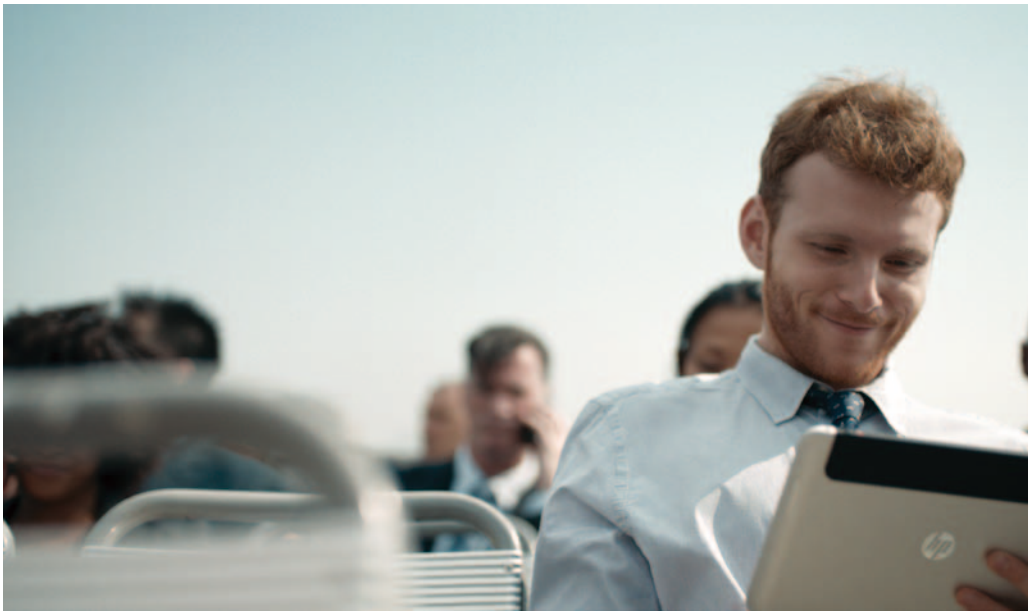
느린 3계층 네트워크
3계층 아키텍처를 사용하는 레거시 네트워크는 유선 액세스를 위해 설계되었습니다. 액세스 스위치는 분산 스위치에 연결된 후 고속 백본에 연결되었습니다. 과거에는 액세스 스위치가 바로 핵심 네트워크에 연결될 수 없었으므로 네트워크가 그렇게 설계될 수밖에 없었습니다. 클라이언트/서버 아키텍처에서 네트워크 관리자는 트래픽을 물리적으로 서로 다른 서브넷으로 분리했습니다.

그러나 현재의 작업 공간 기술은 크게 달라졌습니다. 가상화, 비디오 협업, VoIP(Voice over IP) 및 작업 그룹 협업 같은 고도로 협력적인 기술에는 대기 시간이 짧은 네트워크가 필요합니다. 예를 들어 데이터 및 애플리케이션이 클라우드에 저장되는 데스크탑 가상화의 경우, 사용자에게 애플리케이션이 필요할 때마다 장치를 클라우드 기반 서버에 연결할 수 있어야 합니다. 이전의 3계층 아키텍처에서는 네트워크에 홉(Hop)을 추가해야 했기 때문에 연결 속도가 저하되었습니다.

또한 레거시 무선 네트워크는 적절한 연결을 위한 액세스 포인트에 접근해야 하는 저전력 모바일 장치를 지원하도록 설계되지 않았습니다. 모바일 장치를 적절히 지원하려면 좁은 공간에서 더 많은 장치가 액세스 포인트에 접근할 수 있도록 무선 네트워크를 리-아키텍트하여 밀도를 높여야 합니다.

BYOD를 위한 네트워크 리-아키텍트

BYOD 무선 네트워크를 위한 Best Practice
BYOD가 네트워크에 추가되면서 발생하는 복잡성으로 교착 상태에 빠지는 대신 네트워크를 간소화할 기회를 활용하십시오. 대역폭과 처리량을 높일 수 있는 2계층 네트워크로 네트워크를 리-아키텍트해 보십시오. 소프트웨어 정의 네트워크를 사용하면 사용자로 인해 발생하는 동적 변경을 수용할 수 있도록 네트워크를 쉽게 재구성할 수 있습니다.



2계층 네트워크는 속도가 더 빠르고 대기 시간이 짧기 때문에 비디오 회의 등의 기능이 원활히 작동할 수 있습니다. 2계층 네트워크는 클라우드 서비스와 같이 새로운 유형의 인프라를 지원할 수 있을 정도로 유연하며, 심지어 기존의 투자와 방화벽, 라우팅 및 애플리케이션 딜리버리 최적화 정책도 지원합니다. 애플리케이션 사용 현황부터 라우터 대기 시간에 이르는 모든 정보를 보여주는 단일 인터페이스를 통해 IT 직원의 효율성을 높일 수 있습니다.

유연하고 확장 가능한 네트워크 덕분에 직원은 직장에서 여러 장치를 사용할 수 있습니다. 신규 장치가 추가되고 새로운 비즈니스 요구가 발생함에 따라 확장할 수 있습니다. 또한 유연한 네트워크를 통해 회의실, 구내식당 및 기타 밀도가 높은 공간과 같이 사용자가 많이 모일 수 있는 위치에 액세스 포인트를 쉽게 추가할 수 있습니다. 차세대 WLAN 컨트롤러를 사용하여 이전 컨트롤러에 비해 훨씬 많은 수준인 수천 개에 달하는 액세스 포인트를 관리할 수 있는데, 이는 BYOD를 성공적으로 지원하기 위해 매우 중요한 요소입니다.

네트워크 보안 유지

리-아키텍트된 네트워크를 통해 네트워크 보안을 유지하면서 직장에서 생산성을 높일 수 있는 더 많은 방법을 사용자에게 제공할 수 있습니다. 방법은 다음과 같습니다.

- 게스트가 중요한 부분에 액세스할 수 없도록 네트워크를 분리합니다.
- 네트워크에 연결하는 장치의 유형, 장치에서 실행되는 운영 체제 및 장치에서 사용하는 브라우저를 식별할 수 있는 툴을 배포합니다.
- 802.1X 인증 및 NAC(네트워크 액세스 제어)를 지원하도록 네트워크를 업그레이드합니다. 이렇게 하면 네트워크 관리자가 사용자, 장치 또는 위치에 따라 기업 리소스에 대한 액세스를 제한할 수 있습니다.

유무선 통합 네트워크는 데스크탑 PC를 사용하여 비즈니스 애플리케이션에 액세스하든, 태블릿을 사용하여 비즈니스 애플리케이션에 액세스하든 상관없이 사용자에게 일관된 환경을 제공할 수 있도록 네트워크를 간소화합니다. 간소화된 네트워크를 통해 각각의 관리 플랫폼과 모든 네트워킹 장비의 구성을 수동으로 변경하지 않아도 되도록 자동화할 수 있습니다. 기존 네트워킹 및 보안 투자에 간편하게 통합되므로 단일 플랫폼에서 멀티벤더 인프라를 관리할 수 있습니다.

간소화된 무선 연결

오늘날의 인력은 갈수록 모바일화되고 있으며, 직원들이 자신의 장치를 사용하여 "언제 어디서나" 연결할 수 있기를 원하고 있습니다. 24시간 제공되는 모바일 연결이 필요해짐에 따라 우리가 무선 기술을 바라보는 방식이 바뀌고 있습니다. 이제 무선 기술은 유선 네트워크에 대한 보완책을 넘어서 직원들을 위한 주요 액세스 방법이 되었다고 할 수 있습니다.

유선 네트워크와 같이 빠르고 원활하게 작동하는 무선 액세스에 대한 사용자 요구가 증가하고 있습니다. UCC(통합된 커뮤니케이션 및 공동 작업) 애플리케이션은 모바일 클라이언트에 의해 폭넓게 사용되고 있습니다. 이러한 애플리케이션에는 높은 품질의 음성과 비디오를 위해 향상된 RF(무선 주파수) 범위가 요구됩니다. 이러한 서비스 품질 수준을 충족하려면 802.11ac 액세스 포인트와 함께 제공되는 고성능 무선 LAN이 필요합니다.

무선 네트워크에 IEEE 802.11n보다 이전 표준이 사용된다면 사용자들은 느린 속도 및 애플리케이션 액세스를 경험할 수밖에 없습니다. Wi-Fi 연결을 위한 새로운 802.11ac 액세스 포인트는 무선 연결에 대한 우려를 날려버릴 성능과 보안을 제공합니다. 새로운 802.11ac 액세스 포인트는 설치가 쉽고, SMB의 업무 방식을 가속화하고 능률화하도록 설계된 다양한 기능이 함께 제공됩니다. 최신 802.11ac 기술의 도입으로 이전 표준 대비 최대 3배 빠른 성능을 낼 수 있으며, 내장 관리 대시보드로 손쉽게 관리할 수 있습니다. 새로운 액세스 포인트 기술은 사용자들이 이동하거나 RF 상황이 변경되면 다음과 같이 최적화 작업을 수행합니다.

- 각 모바일 장치가 가장 적합한 액세스 포인트에 연결될 수 있도록 합니다.
- 사용자들이 이동하고 RF 상황이 변경됨에 따라 Wi-Fi 성능을 동적으로 최적화합니다.
- 통합된 무선 침입 보호 기능이 위협에 대한 보호를 제공하여, 별도의 RF 센서나 보안 장비를 도입할 필요가 없어집니다.
- 향상된 품질로 웹 페이지를 보다 빠르게 로드하고 비디오 스트림을 보다 빠르게 제공합니다.
- 고밀도 모바일 장치를 지원합니다.

갈수록 모바일화되는 인력과 고객 기반에 대비해 기업들은 빠르고 안전하게 모바일 장치에 현대적인 애플리케이션을 제공할 수 있어야 합니다. 새로운 802.11ac 액세스 포인트는 미션 크리티컬 애플리케이션 딜리버리 품질을 향상시키고, 고객, 직원, 파트너들에게 향상된 연결을 제공합니다.

결론

HPE BYOD 솔루션은 직원 만족도와 생산성 측면에서 많은 잠재력을 보유하고 있습니다. 레거시 네트워크가 걸림돌이 되도록 두지 마십시오. 현지 비즈니스 파트너나 HPE 영업 대리점에 연락하여 캠퍼스 또는 지사를 위한 BYOD 지원 네트워크를 구축하는 방법을 확인해 보십시오.

자세히 알아보기

hpe.com/networking/byod

4AA4-3882KOP, 2015년 11월, Rev. 1

Hewlett Packard Enterprise