

유·무선 망에서 보안성 강화를 위한 로컬 가상 랜 설계

김영진, 김형진, 조기환*
전북대학교 IT응용시스템학과
*전북대학교 컴퓨터공학부

kyjcom@jbnu.ac.kr, kim@jbnu.ac.kr, ghcho@jbnu.ac.kr

A Local Virtual LAN Design to Enhance Security in Wired and Wireless Networks.

YounGjin kim, HyungJin kim, GiHwan Cho*

Department of IT Applied System Engineering, Chonbuk National University

*Division of Computer Science and Engineering, Chonbuk National University

요 약

업무 효율성을 위한 다양한 비즈니스 환경이 증가하면서 기업의 통신 네트워크도 유·무선이 혼재된 접속환경으로 구성됐다. 이러한 환경에서 대표적인 접근제어 방식으로 정책기반 중앙집중형 네트워크 접근제어 방식과 사용자(스마트기기)기반 네트워크 접근제어 방식이 있다. 하지만 기존의 접근제어 방식은 복잡한 접근 권한 설정과 불필요하게 네트워크 자원을 소모하는 단점이 있다. 본 논문은 유·무선 접속환경에서 로컬 가상 랜 기반 보안성 강화 방안을 제안한다. 제안한 방법은 비즈니스 환경에 따라 네트워크 구성이 가변적인 상황에 최적으로 대응하는 것을 목표로 한다. 유·무선 네트워크에서 유입되는 다양한 IP 패킷은 스위치의 로컬 가상 랜 설정에 따라 2단계 IP 패킷 처리 과정을 거친다. 먼저 스위치는 IP 패킷의 근원에 따라서 유선, 무선, 외부 네트워크로 구분한다. 두 번째 단계로 구분된 IP 패킷에 대한 권한 검증을 통해 내부 네트워크의 중요정보(DB)에 차별하여 접근제어를 한다. 또한 무선 네트워크 및 외부 네트워크로 접속하는 사용자는 가상 사설망(VPN) 기반으로 인증한다. 실험 토폴로지를 통하여 제안기법이 효율적인 네트워크 구성이 가능하고 악의적인 접근에 대한 효과적인 접근제어 및 보안성이 강화됨을 확인한다.

1. 서 론

가상 랜(VLAN: Virtual Local Area Network)이란 물리적 배치에 제한 없이 논리적으로 근거리 네트워크(LAN: Local Area Network)를 구성 가능한 기술이다. 즉 기존에는 근거리 네트워크의 브로드캐스트 도메인을 구분하기 위해 노드들의 용도와 장소별로 별도의 물리적인 장비(스위치)를 사용하여 분리한다. 그러나 가상 랜을 사용하면 사용자의 설정에 따라 네트워크 구성이 가능하다. 노드들의 물리적 위치와 관계없이 노드들을 브로드캐스트 도메인으로 분할 하는 방법으로 논리적인 네트워크 분리가 가능하다. 그리고 서로 다른 가상 랜 사이에는 3계층(Layer 3) 장비를 사용 함으로써 가상 랜끼리 통신이 가능하다.

가상 랜을 네트워크에 적용 시 여러 가지 장점이 있다. 첫째 네트워크 그룹 설정 및 변경을 가상화하여 보안성이 높다. 둘째 논리적인 네트워크의 구분으로 구축비용이 절감된다. 셋째 브로드캐스트 및 멀티캐스트의 효과적인 제어로 불필요한 트래픽을 줄일 수 있다. 넷째 관리자의 네트워크 설정 및 유지보수 작업이 쉬운 장점이 있다.

본 논문에서는 가상 랜의 4가지 구성방식 중에 엔터프라이즈 통신 네트워크 환경에 가장 적합한 로컬 가상 랜 기능을 사용하여 효과적인 접속 경로를 제공하고 보안성을 강화하는 방안을 제안한다. 표 1은 가상 랜의 구성방식의

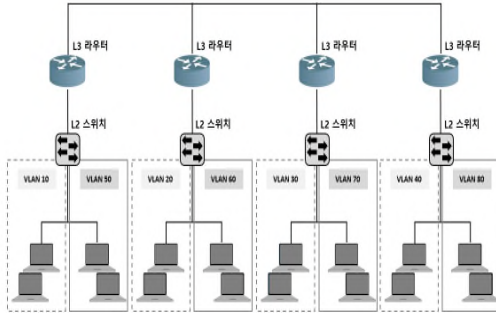
종류 및 특징을 보여준다[1][3].

(표 1) 가상 랜 구성방식의 종류 및 특징

구분	로컬 가상 랜	정책 가상 랜	점 대 점 가상 랜	동적 가상 랜
네트워크 구성 방식	엑세스 계층에 따라 별도 가상 랜으로 분리한다.	포트 주소 기반으로 관리자 가 가상 랜 정보를 직접 설정한다.	사용자 위치에 상관없이 동일 가상 랜을 할당한다.	MAC 주소 기반 가상 랜 프로그램 설정으로 할당한다.
패킷 처리 방식	사용자가 네트워크 이동 시 다른 가상 랜에 접속한다.	노드별 고정 IP를 할당하여 패킷을 처리한다.	가상 랜이 전체 스위치 네트워크에 연결되어 패킷을 처리한다.	프로그램 정책 기반으로 패킷을 처리한다.
장점	네트워크 확장 및 장애처리가 용이하다. (엔터프라이즈망에 권장 함)	노드 장애가 전체 네트워크에 영향이 없다.	동일 가상 랜으로 동일 정책 적용이 용이하다.	VMPS 설정에 따른 가상 랜의 자동설정이 가능하다.
단점	3계층 장비 또는 라우터가 필요하다.	관리자가 모든 포트에 가상 랜 설정 및 관리가 필요하다.	모든 트래픽이 Core를 거쳐야 한다.(엔터프라이즈망에 권장 하지 않음)	VMPS 구축 필요 및 장애 시 모든 서비스가 중단된다.

2. 로컬 가상 랜

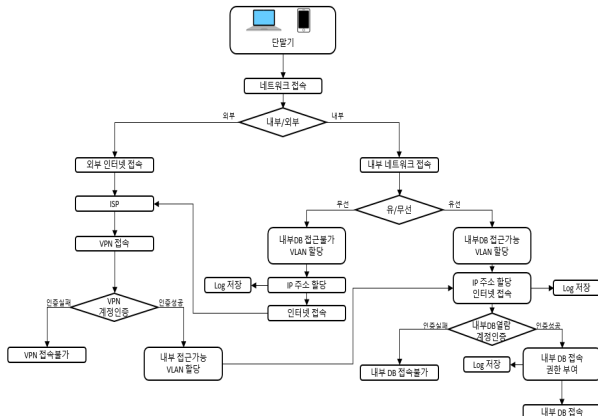
2.1 로컬 가상 랜의 기능 및 설명



(그림 1) 로컬 가상 랜 네트워크 구성도

엑세스 층에 따라 모든 네트워크를 별도의 가상 랜으로 분리하는 방식이며, 3계층 장비(라우터)와 2계층 장비(스위치)를 서로 연결한다. 그리고 라우터의 인터페이스를 논리적으로 분할 하여 각각의 가상 랜을 할당한다. 이처럼 하나의 물리적 인터페이스를 다수의 가상 랜에 소속시키는 것을 트렁킹(Trunking)이라 하고, 해당 포트를 트렁크(Trunk)라고 한다. 엑세스 계층에 따라 네트워크를 별도의 가상 랜으로 분리된 형태이기 때문에 사용자 단말이 물리적인 위치가 이동하게 되면 다른 가상 랜에 소속되게 된다. 로컬 가상 랜을 사용하여 네트워크를 구성하면 네트워크 확장 및 구조변경이 용이하고 이중화 구성이 쉬우며 네트워크 장애시 트래픽 흐름의 예측을 통해 장애 원인 파악 및 조치가 용이하다[2].

2.2 로컬 가상 랜을 사용한 네트워크 접속제어

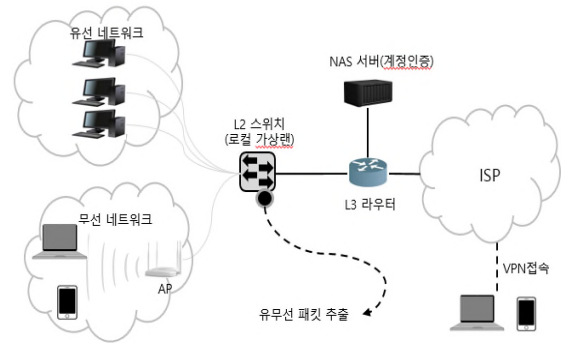


(그림 2) 로컬 가상 랜을 사용한 네트워크 접속제어

유·무선이 혼재된 통신 네트워크 환경에서 다양하게 발생된 유·무선 트래픽에 대하여 2단계 검증과정으로 접근 제어를 수행했다. 첫 번째 단계로 스위치에서 유선, 무선, 외부 네트워크의 IP 패킷을 구분한다. 스위치에 연결되는 유·무선 노드에 따라 유선 가상 랜과 무선 가상 랜을 설정하여 논리적으로 IP 패킷을 구분한다. 이로 인해 스위치를 경유한 IP 패킷은 별도의 정책적용 없이 유·무선 IP 패킷을 구분한다. 두 번째 단계로 구분된 유·무선 IP 패킷에 대한 권한 검증을 통해 내부 네트워크의 중요정보(DB)에 접근제어를 하는 단계로 구분될 수 있다. 또한 무선 및 외부 네트워크로 접속하는 사용자는 가상 사설망(VPN)

기반으로 인증한다. 결과적으로 단말검증과 접근 권한 검증을 통하여 악의적 접근에 대한 보안성을 강화한다. 그리고 사용자가 내부 중요정보(DB)에 접속한 이력이나 IP 주소 할당 후 인터넷에 접속한 로그 정보는 자동으로 저장되며 네트워크 관리자가 보안 관리를 위한 데이터로 사용된다.

2.3 로컬 가상 랜의 실험 네트워크 토폴로지



(그림 3) 로컬 가상 랜 토폴로지

실험 네트워크 토폴로지는 L2 스위치에 유·무선 네트워크 정보를 설정 후 각 설정에 따라 유선 네트워크와 무선 네트워크를 연결하여 구성한다. 그리고 라우터를 사용하여 내부 중요정보(DB)가 저장된 NAS(Network Attached Storage) 서버에 연결한다. 외부 네트워크 사용자는 인터넷서비스제공자(ISP) 망을 경유하고 라우터에서 설정된 가상 사설망(VPN) IP 인증을 통하여 내부 네트워크에 연결된다.

3. 결론

본 연구는 로컬 가상 랜을 사용하여 혼재된 유·무선 접속환경에서 효과적인 접근제어를 위한 방안을 제안한다. 계층 장비(Layer 2)인 스위치의 각 포트에 유무선 네트워크를 구분하여 가상 랜 정보를 미리 설정하고 가상 랜 설정에 따라 2단계 IP 패킷 처리 과정을 거친다. 향후 시뮬레이션 네트워크를 구성하여 유무선 네트워크에서 발생된 다양한 트래픽이 L2 스위치에서 설정된 로컬 가상 랜의 설정에 따라 패킷 접속과 차단 여부를 분석함으로써 본 논문의 우수성을 검증한다.

참고문헌

- [1] 허영일, “엔터프라이즈 환경에서 계정 인증 기반 유·무선 네트워크의 통합 보안 기반구조 구현에 관한 연구,” 부경대학교 일반대학원 기술경영협동과정 학위논문, 2013.
- [2] L. Jiang, H. Tao, X. Yuanming, Z. Jiannan, Y. Richard, L. Yunjie, “VLAN-reusing: A Novel Solution for Efficient Network Virtualization,” Intelligent Automation and Soft Computing, Jan. 2016.
- [3] 이민철, “사용자 역할과 단말기 유형에 따른 802.1X 네트워크의 통합 보안 기반구조 구현과 성능해석,” 한밭대학교 정보통신전문대학원 학위논문, 2015.