VitalQIP 기술자료

DHCP Fingerprint

(DHCP 핑거프린트를 이용한 디바이스 식별 및 접근제어)

Netcurity Inc. (넷큐리티)

CygnaLabs Official Partner

2026년 4월

문서 버전: 1.0 | 대외비

1. 개요

본 문서는 CygnaLabs VitalQIP DDI 솔루션의 DHCP Fingerprint(핑거프린트) 기능에 대한 기술 자료입니다. DHCP Fingerprint는 네트워크에 접속하는 클라이언트 디바이스의 유형과 운영체제를 자동으로 식별하여, 디바이스 기반의 IP 주소 할당 제어 및 보안 정책 적용을 가능하게 하는 기술입니다.

BYOD(Bring Your Own Device) 및 IoT 디바이스의 급격한 증가로 인해, 기존의 MAC 주소 기반 접근제어만으로는 네트워크에 접속하는 다양한 디바이스를 효과적으로 관리하기 어렵습니다. VitalQIP의 DHCP Fingerprint 기능은 이러한 환경에서 디바이스 가시성(Visibility)을 확보하고, 디바이스 유형에 따른 차별화된 네트워크 정책을 자동으로 적용할 수 있는 강력한 솔루션을 제공합니다.

2. DHCP Fingerprint 기술 원리

2.1 DHCP 프로토콜과 핑거프린트

DHCP(Dynamic Host Configuration Protocol)는 네트워크에 접속하는 클라이언트에게 IP 주소와 관련 설정 정보를 자동으로 할당하는 프로토콜입니다. DHCP 통신은 일반적으로 DORA(Discover, Offer, Request, Acknowledge) 과정으로 이루어지며, 이 과정에서 클라이언트는 자신이 필요로 하는 설정 옵션 목록을 서버에 전달합니다.

DHCP Fingerprint는 이 과정에서 클라이언트가 DHCPDISCOVER 메시지에 포함시키는 옵션 정보의 고유한 패턴을 분석하여, 클라이언트의 디바이스 유형 및 운영체제를 식별하는 기술입니다. 각 운영체제와 디바이스 유형은 서로 다른 DHCP 옵션 조합과 순서를 사용하므로, 이 패턴이 일종의 "지문(Fingerprint)"으로 작동합니다.

2.2 핵심 식별 요소

DHCP Fingerprint에서 디바이스 식별에 활용되는 핵심 요소는 다음과 같습니다:

식별 요소	DHCP Option	설명
Parameter Request List	Option 55	클라이언트가 서버에 요청하는 설정 옵션 목록과 그 순서. 핑거프린트의 가장 핵심적인 판별 기준으로, OS별로 고유한 옵션 조합과 순서를 갖습니다.
Vendor Class Identifier	Option 60	클라이언트의 벤더 정보 및 운영체제 버전 등의 추가 정보를 제공합니다. Option 55만으로 구분이 어려운 경우 보조 판별에 활용됩니다.
Client Identifier / MAC OUI	Option 61	클라이언트의 MAC 주소를 통해 네트워크 인터페이스 제조사(OUI)를 확인할 수 있으며, 디바이스 제조사 수준의 식별 정보를 제공합니다.
Host Name	Option 12	클라이언트의 호스트명으로, 공장 초기값을 유지하고 있는 IoT 디바이스 등의 보조 식별에 유용합니다.

2.3 Option 55 (Parameter Request List) 상세

Option 55는 DHCP Fingerprint의 핵심 요소입니다. 클라이언트는 DHCPDISCOVER 또는 DHCPREQUEST 메시지를 보낼 때, 서버로부터 수신하고자 하는 설정 옵션의 번호를 특정 순서대로 나열하여 전송합니다. 이 옵션 번호의 조합과 순서가 각 운영체제 및 디바이스 유형마다 고유하게 나타나므로, 디바이스를 식별하는 효과적인 지표가 됩니다.

OS별 Option 55 핑거프린트 예시

디바이스 / OS	Option 55 시퀀스 (Parameter Request List)
Windows 10/11	1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252
macOS / iOS	1, 121, 3, 6, 15, 119, 252, 95, 44, 46
Linux (Fedora/RHEL 계열)	1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 252, 42
Android	1, 33, 3, 6, 15, 26, 28, 51, 58, 59, 43
VoIP Phone (Grandstream)	1, 3, 6, 12, 15, 42, 43, 66, 67, 120, 125, 150, 160, 161
Samsung Printer	1, 3, 6, 12, 15, 44, 47

위 표에서 보듯이, 동일한 DHCP 프로토콜을 사용하더라도 각 디바이스와 운영체제는 서로 다른 옵션 번호의 조합과 배열 순서를 갖습니다. VitalQIP DHCP 서버는 이러한 패턴을 실시간으로 분석하여 디바이스를 자동 분류합니다.

3. VitalQIP DHCP Fingerprint 기능

3.1 기존 접근제어 방식과의 비교

VitalQIP은 기존에도 다양한 DHCP 접근제어 기능을 제공해 왔습니다. DHCP Fingerprint는 이러한 기존 방식을 보완하고, 특히 BYOD 및 모바일 디바이스에 대한 세밀한 제어를 가능하게 합니다.

접근제어 방식	방식 설명	한계점
MAC Address Pool	특정 MAC 주소 범위에 따라 IP 주소 풀을 지정하여 할당	MAC 주소 스푸핑에 취약하며, 대규모 BYOD 환경에서 관리 부담이 큼
Vendor/User Class	Option 60/77의 Vendor Class 또는 User Class 값에 따른 매칭으로 제어	모든 디바이스가 Vendor Class를 전송하지는 않으며, 값 자체가 변경될 수 있음
Relay Agent (Opt 82)	Circuit ID / Remote ID를 이용한 물리적 위치 기반 접근제어	디바이스 유형이 아닌 접속 위치 기반이므로 BYOD 제어에는 부적합
Access Control (Cache)	Self Registration 또는 CLI로 등록된 MAC 주소를 Cache 서비스로 제어	사전 등록이 필수적이며, 신규 디바이스의 즉시 식별이 불가
DHCP Fingerprint	Option 55의 고유 시그니처 패턴으로 디바이스 유형/OS 자동 식별 및 정책 적용	시그니처 데이터베이스의 지속적 업데이트 필요. 고의적 위변조 가능성 존재

3.2 주요 기능

3.2.1 디바이스 자동 식별 (Automatic Device Identification)

- DHCPDISCOVER 메시지의 Option 55 Parameter Request List 를 실시간 분석하여 클라이언트 디바이스의 유형 및 운영체제를 자동으로 식별합니다.
- Vendor Class Identifier(Option 60), MAC OUI, Host Name 등의 보조 정보를 복합적으로 활용하여 식별 정확도를 극대화합니다.
- 별도의 에이전트 설치 없이, DHCP 트래픽 분석만으로 비침습적(Non-intrusive)인 디바이스 식별이 가능합니다.

3.2.2 정책 기반 접근제어 (Policy-Based Access Control)

- 핑거프린트 매칭 결과에 따라 특정 디바이스 유형에 대해 IP 주소 Lease 를 허용하거나 거부할 수 있습니다.
- 디바이스 유형별로 서로 다른 Scope(주소 범위)에서 IP 주소를 할당하여, 네트워크 세그멘테이션을 자동화할 수 있습니다.
- 디바이스 유형에 맞는 DHCP Option Template 을 자동 적용하여, DHCPOFFER 및 DHCPACK 메시지에 적절한 옵션 값을 전달합니다.

3.2.3 VitalQIP 데이터베이스 연동

- 식별된 DHCP Fingerprint 데이터는 VitalQIP Update Service 를 통해 VitalQIP 중앙 데이터베이스에 자동 기록됩니다.
- 축적된 핑거프린트 데이터를 활용하여 네트워크 자산 검색, 리포트 생성, 디바이스 분포 분석 등의 고급 관리 기능을 활용할 수 있습니다.

4. 동작 흐름

VitalQIP DHCP Fingerprint의 전체 동작 흐름은 다음과 같습니다:

1. **클라이언트 DHCPDISCOVER 전송:** 클라이언트가 네트워크에 접속하면 DHCPDISCOVER 브로드캐스트 메시지를 전송합니다. 이 메시지에는 Option 55(Parameter Request List), Option 60(Vendor Class), Option 12(Host Name) 등의 정보가 포함됩니다.
2. **VitalQIP DHCP 서버의 핑거프린트 분석:** DHCP 서버는 수신한 DHCPDISCOVER 메시지에서 Option 55 의 옵션 번호 목록과 순서를 추출하고, 미리 등록된 핑거프린트 데이터베이스와 매칭합니다.
3. **디바이스 유형 판별:** 매칭 결과를 기반으로 클라이언트 디바이스의 유형(예: Windows PC, iOS 디바이스, VoIP 전화기, IoT 센서 등)을 결정합니다.
4. **접근제어 정책 적용:** 판별된 디바이스 유형에 대해 사전 정의된 접근제어 정책을 적용합니다. Lease 허용/거부, 할당 Scope 결정, DHCP Option Template 지정 등이 이 단계에서 이루어집니다.
5. **DHCPOFFER/DHCPACK 응답:** 정책에 따라 적절한 IP 주소와 옵션 값을 포함한 DHCPOFFER 및 DHCPACK 메시지를 클라이언트에게 전송합니다.
6. **핑거프린트 데이터 기록:** 식별된 핑거프린트 정보는 VitalQIP Update Service 를 통해 중앙 데이터베이스에 저장되어, 이후 검색, 리포트, 감사(Audit) 등에 활용됩니다.

5. 활용 시나리오

5.1 BYOD 환경의 디바이스 분류 및 네트워크 세그멘테이션

기업 네트워크에 접속하는 BYOD 디바이스를 운영체제 유형별(Windows, macOS, iOS, Android 등)로 자동 분류하고, 각 디바이스 유형에 따라 서로 다른 네트워크 세그먼트(VLAN/Scope)에 IP 주소를 할당할 수 있습니다. 예를 들어 회사 업무용 Windows PC에는 내부 업무망 대역을, 개인 모바일 디바이스에는 인터넷 전용 대역을 자동으로 할당하는 것이 가능합니다.

5.2 IoT 디바이스 관리

VoIP 전화기, IP 프린터, CCTV 카메라, 스마트 센서 등 IoT 디바이스는 고유한 DHCP 핑거프린트를 갖습니다. VitalQIP의 DHCP Fingerprint 기능을 통해 이러한 IoT 디바이스를 자동으로 식별하고, 해당 디바이스에 적합한 TFTP 서버(Option 66), Boot File(Option 67) 등의 전용 설정을 자동 배포할 수 있습니다.

5.3 비인가 디바이스 탐지 및 차단

핑거프린트 데이터베이스에 등록되지 않은 미지의 디바이스가 네트워크에 접속을 시도할 경우, 이를 탐지하고 Lease를 거부하거나 격리 네트워크로 유도할 수 있습니다. 이를 통해 비인가 디바이스에 대한 선제적 보안 대응이 가능합니다.

5.4 네트워크 자산 가시성 확보 및 감사

VitalQIP 데이터베이스에 축적된 핑거프린트 데이터를 활용하여, 네트워크에 접속하는 전체 디바이스의 유형별 분포를 파악하고, 디바이스 인벤토리 관리 및 보안 감사(Audit) 리포트를 생성할 수 있습니다.

6. 구성 개요

6.1 핑거프린트 정의

VitalQIP에서 DHCP Fingerprint를 활용하기 위해서는 먼저 식별 대상이 되는 디바이스의 핑거프린트 시그니처를 정의해야 합니다. 핑거프린트는 Option 55의 옵션 번호 시퀀스를 기반으로 하며, 필요에 따라 Option 60(Vendor Class Identifier) 등의 보조 조건을 추가로 설정할 수 있습니다.

6.2 Client Class 연동

정의된 핑거프린트는 VitalQIP의 Client Class 기능과 연동됩니다. Client Class는 특정 조건을 만족하는 DHCP 클라이언트에게 차별화된 DHCP 옵션 템플릿이나 정책을 적용할 수 있는 VitalQIP의 핵심 기능으로, Vendor Class 및 User Class 기반의 기존 Client Class 메커니즘에 핑거프린트 기반의 매칭 조건이 추가된 형태입니다.

6.3 Scope/Range 할당 정책

핑거프린트 매칭 결과에 따라 특정 디바이스 유형을 특정 Scope(주소 범위)로 매핑할 수 있습니다. 이를 통해 디바이스 유형별 네트워크 분리 정책을 DHCP 수준에서 자동으로 적용할 수 있으며, 별도의

NAC(Network Access Control) 장비 없이도 기본적인 디바이스 기반 세그멘테이션이 가능합니다.

6.4 DHCP Option Template 적용

핑거프린트로 식별된 디바이스 유형에 따라 서로 다른 DHCP Option Template을 자동으로 적용할 수 있습니다. 예를 들어 VoIP 전화기로 식별된 디바이스에게는 TFTP 서버 주소와 Boot File 경로를 포함한 전용 템플릿을, 일반 PC에게는 DNS 서버와 도메인 정보가 포함된 표준 템플릿을 각각 적용합니다.

6.5 DHCP Generation 및 배포

핑거프린트 관련 설정이 완료되면, VitalQIP DHCP Generation을 통해 설정 파일을 생성하고 DHCP 서버에 배포합니다. VitalQIP GUI(웹 클라이언트 또는 CLI)에서 DHCP > DHCP Servers > DHCP Generation 메뉴를 통해 설정 파일의 미리보기(Preview) 및 서버 푸시(Push to Server)를 수행할 수 있습니다.

7. 유의사항 및 베스트 프랙티스

1. **핑거프린트 데이터베이스 관리:** DHCP Fingerprint 의 정확도는 핑거프린트 시그니처 데이터베이스의 품질과 최신성에 직접적으로 의존합니다. 새로운 디바이스 유형 및 OS 버전이 출시될 때마다 핑거프린트 데이터베이스를 지속적으로 업데이트해야 합니다. Fingerbank(www.fingerbank.org) 등의 커뮤니티 데이터베이스를 참고하여 최신 핑거프린트 정보를 반영하는 것을 권장합니다.
2. **보안 한계 인식:** DHCP Fingerprint 는 클라이언트가 전송하는 DHCP 패킷의 내용을 분석하는 방식이므로, 의도적으로 DHCP 옵션을 위변조(spoofing)하는 공격에는 취약할 수 있습니다. 따라서 DHCP Fingerprint 는 완전한 보안 솔루션이 아닌, 디바이스 가시성 확보 및 접근제어의 보조 수단으로 활용하는 것이 적절합니다. 802.1X 인증, NAC 등의 기존 보안 체계와 병행 운용하는 것을 권장합니다.
3. **정적 IP 디바이스 제외:** DHCP Fingerprint 는 DHCP 를 통해 IP 주소를 할당받는 디바이스에만 적용됩니다. 정적 IP 주소를 사용하거나 VPN, 프록시를 경유하여 DHCP 과정을 우회하는 디바이스에 대해서는 핑거프린트 기반 식별이 불가합니다.
4. **다중 인터페이스 디바이스:** 유선과 무선 인터페이스를 동시에 사용하는 디바이스의 경우, 각 인터페이스별로 서로 다른 핑거프린트가 생성될 수 있으므로 이를 감안한 정책 설계가 필요합니다.
5. **단계적 적용:** 초기 도입 시에는 모니터링 모드로 운용하여 핑거프린트 데이터를 충분히 수집하고 분석한 후, 단계적으로 접근제어 정책을 적용하는 것을 권장합니다. 갑작스러운 차단 정책 적용은 정상 디바이스의 네트워크 접속에 영향을 줄 수 있습니다.

8. 타사 제품 대비 VitalQIP 차별점

항목	VitalQIP (CygnaLabs)	Infoblox	일반 DHCP 서버
Fingerprint 지원	Option 55 기반 시그니처 매칭 + Option 60/MAC OUI 보조 식별	DHCP Fingerprint Detection 지원	기본 미지원 또는 제한적
접근제어 연동	Client Class, Scope 할당, Option Template 연동으로 자동 정책 적용	Fingerprint 기반 필터링 가능	수동 설정 필요
DB 연동 및 리포트	VitalQIP 중앙 DB에 자동 기록, 검색 및 리포트 기능 제공	Grid DB 연동 및 리포트	별도 로그 분석 필요
DDI 통합 관리	DNS, DHCP, IPAM 통합 관리 플랫폼에서 일원화된 핑거프린트 관리	통합 DDI 플랫폼	DHCP 기능만 단독 제공
확장성	대규모 엔터프라이즈 환경에 최적화된 분산 아키텍처	Grid 기반 분산 구성	제한적

9. 결론

VitalQIP의 DHCP Fingerprint 기능은 별도의 에이전트 설치나 네트워크 인프라 변경 없이, 기존 DHCP 인프라를 활용하여 네트워크에 접속하는 모든 디바이스의 유형과 운영체제를 자동으로 식별할 수 있는 강력한 기능입니다.

BYOD 확산, IoT 디바이스 증가, 보안 위협 고도화 등 현대 엔터프라이즈 네트워크 환경의 핵심 과제에 대응하기 위해, DHCP Fingerprint를 통한 디바이스 가시성 확보와 정책 기반 접근제어는 필수적인 요소입니다. VitalQIP의 DDI 통합 관리 플랫폼과 결합된 DHCP Fingerprint는 기업 네트워크의 보안성과 관리 효율성을 동시에 강화할 수 있는 최적의 솔루션입니다.

문의처

Netcurity Inc. (넷큐리티) | CygnaLabs Official Partner

본 문서에 대한 추가 기술 문의 또는 PoC(Proof of Concept) 요청은 넷큐리티 기술영업팀으로 연락 부탁드립니다.