

Catalyst 5000 EARL 버전 및 기타 일반적인 EARL 질문 확인

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[백작이 뭐야?](#)

[CLI에서 EARL 버전 확인](#)

[부품 번호 매트릭스에서 EARL 버전 확인](#)

[Modular Supervisor Catalyst 5000 Series Supervisor](#)

[고정 구성 Catalyst 5000 Series 스위치](#)

[SNMP를 통해 EARL 버전 확인](#)

[Catalyst 5000 EARL 1 버전만 영향을 받는 이유는 무엇입니까?](#)

[네트워크에 STP 이중화가 없는 경우 계속 업그레이드해야 합니까?](#)

[802.1x 취약성의 영향을 받지 않는 Catalyst 4000 및 6000](#)

[Windows 2000 802.1x 참여](#)

[관련 정보](#)

[소개](#)

이 문서에서는 Catalyst 5000 스위치의 802.1x 취약성 문제와 관련된 일반적인 질문을 다룹니다. 이 문서에는 Catalyst 5000 EARL 버전을 확인하는 방법도 나와 있습니다. 802.1x 취약성에 대한 자세한 내용은 다음 보안 권고 사항을 참조하십시오.

<http://www.cisco.com/warp/public/707/cisco-sa-20010413-cat5k-8021x.shtml>

[사전 요구 사항](#)

[요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

[사용되는 구성 요소](#)

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

백작이 뭐야?

Encoded Address Recognition Logic(EARL)은 Catalyst 5000 Supervisor Engine의 MAC 주소를 기반으로 패킷을 학습하고 전달하는 중앙 집중식 처리 엔진입니다.EARL은 VLAN, MAC 주소 및 포트 관계를 저장합니다.이러한 관계는 하드웨어에서 스위칭 결정을 내리는 데 사용됩니다.

CLI에서 EARL 버전 확인

CLI(Command Line Interface)에서 EARL 버전을 확인하려면 Supervisor에서 **show module** 명령을 실행합니다.다음은 예입니다.

```
Console (enable) sh mod
Mod Module-Name Ports Module-Type Model Serial-Num Status
-----
1 2 100BaseFX MM Supervis WS-X5506 005441962 ok
2 48 10BaseT Ethernet WS-X5012A 010308246 ok
3 48 10BaseT Ethernet WS-X5012A 010308178 ok
4 24 3 Segment 100BaseTX E WS-X5223 005389389 ok
5 12 100BaseFX MM Ethernet WS-X5201R 008951252 ok

Mod MAC-Address(es) Hw Fw Sw
-----
1 00-e0-f9-d6-64-00 to 00-e0-f9-d6-67-ff 1.0 2.2(2) 4.2(1)
2 00-90-6f-6e-75-c0 to 00-90-6f-6e-75-ef 1.0 4.2(1) 4.2(1)
3 00-90-6f-6e-5a-f0 to 00-90-6f-6e-5b-1f 1.0 4.2(1) 4.2(1)
4 00-e0-b0-fb-0a-29 to 00-e0-b0-fb-0a-2b 1.0 2.2(1) 4.2(1)
5 00-60-2f-39-3d-d4 to 00-60-2f-39-3d-df 1.1 4.1(1) 4.2(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1 EARL 1+ WS-F5511 0005442554 1.0
```

위에서 Supervisor에서 실행한 **show module** 명령은 Sub-Type 필드에 EARL Hardware Version을 표시합니다.Supervisor가 EARL 1, 1.1 또는 1+,1++이면 시스템은 802.1x 취약성의 영향을 받습니다.NFFC, NFFC+ 또는 NFFC II와 같은 하위 유형에 지정된 EARL의 다른 버전은 EARL 1이 아니며 802.1x 취약성의 영향을 받지 않습니다.

참고: 슈퍼바이저 IIG 및 IIG는 하위 유형을 인쇄하지 않습니다.Supervisor IIG 및 IIG는 EARL 3이며 802.1x 취약성의 영향을 받지 않습니다.

부품 번호 매트릭스에서 EARL 버전 확인

Modular Supervisor Catalyst 5000 Series Supervisor

슈퍼바이저	슈퍼바이	얼 버전	EARL 버	802.1x 취
-------	------	------	--------	----------

부품 번호	저 모델	하위 유형	전 하위 모델 유형	약성의 영향
WS-X5005	수퍼바이저 I	백작 1	WS-F5510	예
WS-X5006	수퍼바이저 I	백작 1	WS-F5510	예
WS-X5009	수퍼바이저 I	백작 1	WS-F5510	예
WS-X5505	수퍼바이저 II	1 이상 백작	WS-F5511	예
WS-X5506	수퍼바이저 II	1 이상 백작	WS-F5511	예
WS-X5509	수퍼바이저 II	1 이상 백작	WS-F5511	예
WS-X5530-E1	수퍼바이저 III	EARL 1++	WS-F5520	예
WS-X5530-E2	수퍼바이저 III NFFC	얼 2(NFFC)	WS-F5521	아니요
WS-X5530-E2A	수퍼바이저 III NFFC-A	얼 2(NFFC)	WS-F5521	아니요
WS-X5530-E3	수퍼바이저 III NFFC II	얼 3 (NFFC II)	WS-F5531	아니요
WS-X5530-E3A	수퍼바이저 III NFFC II-A	얼 3 (NFFC II)	WS-F5531	아니요
WS-X5534	수퍼바이저 III F	EARL 1++	WS-F5520	예
WS-X5540	수퍼바이저 II G	얼 3 (NFFC II)	WS-F5531	아니요
WS-X5550	수퍼바이저 III G	얼 3 (NFFC II)	WS-F5531	아니요

고정 구성 Catalyst 5000 Series 스위치

스위치 부품 번호	수퍼바이저 모델	얼 버전 하위 유형	EARL 버전 하위 모델 유형	802.1x 취약성의 영향
WS-C2901	수퍼바이저 I	백작 1	WS-F5510	예
WS-C2902	수퍼바이저 I	백작 1	WS-F5510	예

WS-C2926T	수퍼바이저 II	1 이상 백작	WS-F5511	예
WS-C2926G	수퍼바이저 II	1 이상 백작	WS-F5511	예
WS-C2926GS	수퍼바이저 III NFFC II	얼 3 (NFFC II)	WS-F5531	아니요
WS-C2926GL	수퍼바이저 III NFFC II	얼 3 (NFFC II)	WS-F5531	아니요

참고: 초기 소프트웨어 개정에서는 NSF 3(NFFC II)을 NFFC+라고 할 수 있습니다.

SNMP를 통해 EARL 버전 확인

EARL 하드웨어 버전은 SNMP(Simple Network Management Protocol)에 의해 결정됩니다.
.iso.org.dod.internet.private.enterprises.cisco.workgroup.stack.moduleGrp.mo 사용

moduleTable.moduleEntry.module하위 유형

.1.3.6.1.4.1.9.5.1.3.1.1.16

반환 값은 다음과 같습니다.

- 기타(1)
- 비어 있음(2)
- wsf5510(3) (EARL1)
- wsf5511(4) (EARL1+)
- wsx5304(6) (RSM—NOT ON SUPERVISOR)
- wsf5520(7) (EARL1+)
- wsf5521(8) (EARL2/NFFC)
- wsf5531(9) (EARL3/NFFCII)

Supervisor II G 및 IIG는 값을 반환하지 않습니다. Supervisor IIG 및 IIG는 EARL 3이며 802.1x 취약성의 영향을 받지 않습니다.

Catalyst 5000 EARL 1 버전만 영향을 받는 이유는 무엇입니까?

EARL 1 버전은 예약된 각 MAC 주소에 대해 EARL 1을 개별적으로 프로그래밍해야 하므로 만 영향을 받습니다. 다른 모든 EARL 버전은 범위로 프로그래밍되었으므로 802.1x 프레임을 전달하지 않습니다.

네트워크에 STP 이중화가 없는 경우 계속 업그레이드해야 합니까?

물론 Catalyst 5000 소프트웨어는 여전히 모든 포트에서 패킷을 전달합니다. 스위치에서 인바운드

되는 프레임을 삭제해야 합니다.STP 이중화가 없는 한 네트워크가 성능 저하를 겪지는 않지만 스위치가 여전히 제대로 작동하지 않습니다.

802.1x 취약성의 영향을 받지 않는 Catalyst 4000 및 6000

Catalyst 5000 Series 스위치(EARL 1 포함)는 유일하게 영향을 받는 스위치입니다.다른 모든 스위치는 프레임을 포워딩하지 않으며 스위치가 STP 경로에 있으면 STP 루프가 발생하지 않도록 실제로 중지합니다.

Windows 2000 802.1x 참여

현재 Windows XP(Whistler)는 802.1x를 지원하는 유일한 Microsoft 운영 체제입니다.Microsoft에 따르면 나중에 소프트웨어 업그레이드 또는 패치를 통해 Windows 2000용 802.1x를 추가할 수 있습니다.현재 Windows XP(Whistler)는 802.1x를 지원하는 유일한 Microsoft 운영 체제입니다 .Microsoft에 따르면 Windows 2000용 802.1x는 나중에 소프트웨어 업그레이드 또는 패치를 통해 추가될 수 있습니다.

관련 정보

- [Catalyst 5000 제품군 소프트웨어 릴리스 4.x 릴리스 정보](#)
- [기술 지원 및 문서 - Cisco Systems](#)