기술 세부사항

네트워크 프로토콜

Cisco IP Conference Phone 8832는 음성 통신에 필요한 몇 개의 업계 표준과 Cisco 네트워크 프로토콜을 지원합니다. 다음 표에는 전화기에서 지원하는 네트워크 프로토콜에 대한 개요가 나와 있습니다.

표 ***1: Cisco IP*** 전화회의 전화기에서 지원하는 네트워크 프로토콜

네트워크 프로토콜	목적	사용 참고 사항
BootP(Bootstrap Protocol)	BootP는 전화기 같은 네트워크 장치를 활성화하여 IP 주소와 같은 특정 시작 정보를 확인합니다.	—
CDP (Cisco 탐색 프로토콜)	CDP는 모든 Cisco 제조 장비에서 실행되는 장치 검색 프로토콜입니다. 장치는 CDP를 사용하여 해당 장치의 존재 여부를 다른 장치에 알리고 네트워크에 있는 다른 장치에 대한 정보를 수신할 수 있습니다.	전화기는 CDP를 사용해 Cisco Catalyst 스위치 구성 정보 같은 정보를 주고 받을 수 있습니다
DHCP(Dynamic Host Configuration Protocol)	DHCP는 네트워크 장치에 IP 주소를 역동적으로 할당합니다. DHCP를 사용하면 네트워크에 IP 전화기를 연결하고, 수동으로 IP 주소를 할당하거나 추가 네트워크 매개변수를 구성하지 않고도 전화기를 작동시킬 수 있습니다.	DHCP는 기본값으로 활성화됩니다. 비활성화 TFTP 서버를 수동으로 구성해야 합니다. DHCP 사용자 정의 옵션 150을 사용할 것을 권 지원되는 DHCP 구성에 관한 자세한 내용은 참고 옵션 150을 사용할 수 없다면, DHCP

기술 세부사항

네트워크 프로토콜	목적	사용 참고 사항
HTTP(Hypertext Transfer Protocol)	HTTP는 인터넷 및 웹 상에서 정보 교환 및 문서 이동을 위해 사용하는 표준 프로토콜입니다.	전화기는 XML 서비스, 프로비저닝, 업그레이드
HTTPS(Hypertext Transfer Protocol Secure)	HTTPS(Hypertext Transfer Protocol Secure)는 HTTP(Hypertext Transfer Protocol)와 SSL/TLS 프로토콜의 조합으로 서버에 암호화 및 보안 식별 기능을 제공합니다.	HTTP와 HTTPS가 모두 지원되는 웹 애플리케이 URL을 선택합니다. 서비스에 대한 연결이 HTTPS를 통해 이루어지
IEEE 802.1X	IEEE 802.1X 표준은 클라이언트 서버 기반 액세스 제어 및 개방형 액세스 포트를 통한 LAN 연결에서 인증받지 못한 클라이언트를 제한하는 인증 프로토콜을 정의합니다. 클라이언트가 인증될 때까지, 802.1X 액세스 제어는 클라이언트가 연결된 포트를 통해 오직 EAPOL(Extensible Authentication Protocol over LAN) 트래픽만 허용합니다. 인증에 성공하면 정상적인 트래픽은 포트를 통과할 수 있습니다.	전화기는 EAP-FAST 및 EAP-TLS라는 인증 방식 전화기에서 802.1X 인증이 활성화되면, 음성 VL
IP(Internet Protocol)	IP는 네트워크를 통해 패킷을 처리하고 전송하는 메시징 프로토콜입니다.	IP로 통신하기 위해서는 네트워크 장치에 IP 주 IP 주소, 서브넷 및 게이트웨이 ID는 전화기에서 으로 할당됩니다. DHCP를 사용하지 않는다면 로 전화기는 IPv6 주소를 지원합니다. 자세한 내용은 시오.
LLDP(Link Layer Discovery Protocol)	LLDP는 일부 Cisco 및 타사 장치에서 지원되는 표준화된 네트워크 검색 프로토콜(CDP와 유사)입니다.	전화기는 PC 포트에서 LLDP를 지원합니다.
LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED는 음성 제품을 위해 개발된 LLDP 확장 표준입니다.	전화기는 다음과 같은 정보를 주고받기 위해 SW • 음성 VLAN 구성 • 장치 검색 • 전력 관리 • 재고 관리 LLDP-MED 지원에 대한 자세한 내용은 다음 UR https://www.cisco.com/en/US/tech/tk652/tk701/tech
RTP(Real-Time Transport Protocol)	RTP는 데이터 네트워크상에서 대화형 음성 및 비디오 같은 실시간 데이터를 전송하기 위한 표준 프로토콜입니다.	전화기는 RTP 프로토콜을 사용해 기타 전화기 및
RTCP(Real-Time Control Protocol)	RTCP는 RTP와 함께 작동하여 RTP 스트림에 대한 QoS 데이터(예: 지터, 대기 시간 및 왕복 지연) 를 제공합니다.	RTCP는 기본적으로 활성화됩니다.

네트워크 프로토콜	목적	사용 참고 사항
SDP(Session Description Protocol)	SDP는 두 엔드포인트 간 연결 중 사용할 수 있는 매개 변수를 판별하는 SIP 프로토콜의 부분입니다. 전화회의는 전화회의의 모든 엔드포인트가 지원하는 SDP 기능만을 사용하여 설정됩니다.	코덱 유형, DTMF 탐지 및 통신 소음과 같은 S 는 Media Gateway에 의해 전역으로 구성됩니 성을 허용할 수 있습니다.
SIP(Session Initiation Protocol)	SIP는 IP를 통해 멀티미디어 전화 회의를 진행할 때 사용하는 인터넷 IETF(Engineering Task Force) 표준입니다. SIP는 2개 이상의 엔드포인트 간에 통화를 연결, 유지, 종료할 때 사용할 수 있는 ASCII 기반의 애플리케이션 레이어 프로토콜(RFC 3261 정의 내용)입니다.	다른 VoIP 프로토콜처럼 SIP도 패킷 텔레포니 다. 시그널링을 통해 통화 정보는 네트워크 경 니다.
SRTP(Secure Real-Time Transfer protocol)	SRTP는 RTP(Real-Time Protocol) 음성/비디오 프로파일이 확장된 것으로, 두 엔드포인트를 이동하는 미디어 패킷의 인증, 무결성 및 암호화를 제공하여 RTP와 RTCP(Real-Time Control Protocol) 패킷의 무결성을 보장합니다.	전화기는 미디어 암호화를 위해 SRTP를 사용
TCP(Transmission Control Protocol)	TCP는 연결 지향형 전송 프로토콜입니다.	전화기는 TCP를 사용하여 Cisco Unified Com
TLS(Transport Layer Security)	TLS는 통신 보안 및 인증을 위한 표준 프로토콜입니다.	보안이 시행될 때, 전화기는 Cisco Unified Co 자세한 내용은 해당 Cisco Unified Communica
TFTP(Trivial File Transfer Protocol)	TFTP를 사용하면 네트워크상에서 파일을 전송할 수 있습니다. 전화기에서 TFTP는 전화기 유형에 맞는 구성 파일을 확보할 수 있게 해줍니다.	TFTP는 네트워크에 TFTP 서버를 요구하고, 가 지정한 것이 아닌 다른 TFTP 서버를 사용 수동으로 할당해야 합니다. 자세한 내용은 해당 Cisco Unified Communica
사용자 데이터그램 프로토콜	UDP는 데이터 패킷 전달을 위한 연결 메시징 프로토콜입니다.	UDP는 RTP 스트림에만 사용됩니다. 전화기

네트워크 혼잡 시 전화기 동작

네트워크 성능을 저하시키는 것이라면 무엇이나 전화기 오디오에 영향을 미칠 수 있고, 어떤 경우에는 통화가 끊어지게 만들 수도 있습니다. 네트워크 저하의 근원에는 다음과 같은 활동이 포함되며 이에 국한되는 것은 아닙니다.

- 관리자 작업(예: 내부 포트 스캔 또는 보안 스캔)
- 네트워크에 발생한 공격(예: DoS(서비스 거부) 공격 등)

SIP 및 NAT 구성

SIP 및 Cisco IP 전화기

Cisco IP 전화기는 세션 시작 프로토콜(SIP)을 사용하며 이를 통해 SIP를 지원하는 모든 IT 서비스 제공자와 상호 운용할 수 있습니다. SIP는 IP 네트워크에서 음성 통신 세션을 제어하는 IETF 정의 신호 처리 프로토콜입니다.

SIP는 패킷 전화 통신 네트워크 내에서 신호 및 세션 관리를 처리합니다. 시그널링을 통해 통화 정보는 네트워크 경계로 이동됩니다. 세션 관리 는 엔드 투 엔드 통화의 특성을 제어합니다.

일반적인 상용 IP 전화 통신 구축에서 모든 통화는 SIP 프록시 서버를 통해 이동합니다. 요청 전화기를 사용자 에이전트 클라이언트(UAC)라고 하고 수신 전화기를 SIP 사용자 에이전트 서버(UAS)라고 합니다.

SIP 메시지 라우팅은 동적입니다. SIP 프록시가 연결을 위해 UAS로부터의 요청을 수신하지만 UAC를 검색할 수 없는 경우 프록시는 네트워크 내의 다른 SIP 프록시로 메시지를 전달합니다. UAC가 검색되면 UAS로 응답이 다시 전달되고 다이렉트 P2P 세션을 사용하여 2개의 UA가 연결됩니다. 음성 트래픽은 실시간 프로토콜(RTP)를 사용하여 동적으로 지정된 포트에서 UA 사이에 전송됩니다.

RTP는 오디오 및 비디오 등의 실시간 데이터는 전송하지만 RTP는 데이터의 실시간 전송을 보장하지 않습니다. RTP는 전송 및 수신 애플리케이션에 대한 매커니즘을 제공하여 스트리밍 데이터를 지원합니다. 일반적으로, RTP는 UDP 위에서 실행됩니다.

SIP Over TCP

상태 기반 통신을 보장하기 위해 Cisco IP 전화기는 TCP를 SIP용 전송 프로토콜로 사용합니다. 이 프로토콜은 보장 배달을 제공하여 손실된 패킷이 재전송됩니다. 또한, TCP는 SIP 패키지가 전송된 동일한 순서로 수신되는 것을 보장합니다.

TCP는 기업 방화벽에 의한 UDP 포트 차단 문제를 해결합니다. TCP는 인터넷 브라우징 또는 전자 상거래 등과 같이 이미 기본 활동으로 사용 중이므로 TCP를 사용하면 새 포트를 열 필요가 없거나 패킷이 손실되지 않습니다.

SIP 프록시 중복

평균적인 SIP 프록시 서버는 수만 명의 가입자를 처리할 수 있습니다. 백업 서버를 사용하면 유지 보수를 위해 일시적으로 활성 서버를 끌 수 있습니다. 전화기는 서비스 중단을 최소화하거나 제거하기 위해 백업 서버 사용을 지원합니다.

프록시 중복을 제공하는 간단한 방법은 전화기 구성 프로파일에 SIP 프록시 서버를 지정하는 것입니다. 전화기가 DNS NAPTR 또는 SRV 쿼리를 DNS 서버로 전송합니다. 구성된 경우 DNS 서버는 호스트 이름, 우선 순위, 대기 포트 등 도메인에 대한 서버 목록을 포함하는 SRV 기록을 반환합니다. 전화기는 우선 순위대로 호스트와의 접촉을 시도합니다. 번호가 낮은 서버의 우선 순위가 더 높습니다. 쿼리에서 최대 6개의 NAPTR 레코드 및 최대 12개의 SRV 레코드가 지원됩니다.

전화기가 기본 서버와 통신 하는 데 실패할 경우, 전화기는 우선 순위가 더 낮은 서버로 장애 조치될 수 있습니다. 구성된 경우 전화기에서 기본으로 다시 연결을 복원할 수 있습니다. 장애 조치 및 장애

복구 지원은 SIP 전송 프로토콜이 서로 다른 서버 간에 전환됩니다. 통화가 종료되고 장애 복구 조건이 충족될 때까지 전화기는 활성 통화 중에 기본 서버에 대한 장애 복구를 수행하지 않습니다.

DNS 서버에 있는 리소스 레코드의 예

```
as1bsoft      3600    IN NAPTR 50   50  "s"  "SIPS+D2T"     ""  _sips._tcp.tlstest
              3600    IN NAPTR 90   50  "s"  "SIP+D2T"      ""  _sip._tcp.tcptest
              3600    IN NAPTR 100  50  "s"  "SIP+D2U"      ""  _sip._udp.udptest

_sips._tcp.tlstest  SRV 1 10 5061 srv1.sipurash.com.
                    SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest   SRV 1 10 5061 srv3.sipurash.com.
                    SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest   SRV 1 10 5061 srv5.sipurash.com.
                    SRV 2 10 5060 srv6.sipurash.com.

srv1      3600    IN    A   1.1.1.1
srv2      3600    IN    A   2.2.2.2
srv3      3600    IN    A   3.3.3.3
srv4      3600    IN    A   4.4.4.4
srv5      3600    IN    A   5.5.5.5
srv6      3600    IN    A   6.6.6.6
```

다음 예는 전화기의 관점에서 서버의 우선 순위를 보여줍니다.

```
Priority        IP Address      SIP Protocol    Status
1st             1.1.1.1             TLS            UP
2nd             2.2.2.2             TLS            UP
3rd             3.3.3.3             TCP            UP
4th             4.4.4.4             TCP            UP
5th             5.5.5.5             UDP            UP
6th             6.6.6.6             UDP            UP
```

전화기는 항상 우선 순위가 가장 높은 사용 가능한 주소로 SIP 메시지를 보내며 목록의 UP 상태를 표시합니다. 이 예에서 전화기는 모든 SIP 메시지를 주소 1.1.1.1로 전송합니다. 목록의 주소 1.1.1.1 상태가 DOWN으로 표시된 경우 전화기가 대신 2.2.2.2와 통신합니다. 지정된 장애 복구 조건이 충족되면 전화기에서 1.1.1.1으로 다시 연결을 복원할 수 있습니다. 페일오버 및 장애 복구에 대 한 자세한 내용은 SIP 프록시 페일오버, 5 페이지 및 SIP 프록시 폴백, 6 페이지의 내용을 참조하십시오.

SIP 프록시 페일오버

전화기는 다음과 같은 경우에 장애 조치를 수행합니다.

- 전화기가 SIP 메시지를 전송하고 서버에서 응답하지 않습니다.
- 서버에서 **Backup RSC** 시도 중 지정된 코드와 일치하는 코드를 사용하여 응답합니다.
- 전화기에서 TCP 연결 끊기 요청을 가져옵니다.

SIP 전송이 자동으로 설정된 경우 대체 작동 시 자동 등록을 예로 설정하는 것이 좋습니다.

구성 파일에서 이 확장자별 매개 변수를 구성할 수도 있습니다.

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
<Auto_Register_When_Failover_n_ ua="na">Yes</Auto_Register_When_Failover_n_>
```

여기서 *n*은 내선 번호입니다.

전화기 대체 작동 동작

전화기가 현재 연결된 서버와 통신하는 데 실패하면 서버 목록 상태를 새로 고칩니다. 사용할 수 없는 서버가 서버 목록에 DOWN 상태로 표시되어 있습니다. 전화기가 목록에서 상태가 UP인 최상위 서버에 연결을 시도합니다.

다음 예에서는 주소 1.1.1.1 및 2.2.2.2를 사용할 수 없습니다. 전화기가 3.3.3.3에 SIP 메시지를 전송합니다 .이 서버는 상태가 UP인 서버 중에서 우선 순위가 가장 높습니다.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

다음 예에서는 DNS NAPTR 응답에 두 개의 SRV 레코드가 있습니다. 각 SRV 레코드에는 3 개의 A 레코드(IP 주소)가 있습니다.

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

전화기가 1.1.1.1에 연결되지 않아 1.1.1.2에 등록 된 것으로 가정해 보겠습니다. 1.1.1.2가 다운되면 전화기 동작은 프록시 폴백 간격의 설정에 따라 달라집니다.

- 프록시 폴백 간격이 **0**으로 설정된 경우 전화기는 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3 주소 순서로 시도합니다.
- 프록시 폴백 간격가 0이 아닌 값으로 설정된 경우 전화기는 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3 주소 순서로 시도합니다.

SIP 프록시 폴백

프록시 대체에는 전화기 웹 인터페이스의 내선 번호**(n)** 탭에 있는 프록시 대체 간격 필드에 지정된 0 이 아닌 값이 필요합니다. 이 필드를 0으로 설정하면 SIP 프록시 장애 복구 기능이 비활성화 됩니다. 구성 파일에서 이 확장자별 매개 변수를 다음과 같은 형식으로 구성할 수도 있습니다.

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
```

여기서 *n*은 내선 번호입니다.

전화기가 장애 복구를 트리거하는 시간은 사용 중인 전화기 구성 및 SIP 전송 프로토콜에 따라 달라집니다.

서로 다른 SIP 전송 프로토콜 사이에서 장애 복구를 수행하도록 전화기를 활성화하려면 전화기 웹 인터페이스의 내선 번호**(n)** 탭에서 **SIP** 전송을 자동으로 설정합니다. 구성 파일에서 이 확장자별 매개변수를 다음 XML 문자열을 사용하여 구성할 수도 있습니다.

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

여기서 *n*은 내선 번호입니다.

UDP 연결에서 장애 복구

UDP 연결에서 장애 복구는 SIP 메시지에 의해 트리거됩니다. 다음 예에서는 서버로부터 응답이 없으므로 전화기가 T1에 1.1.1.1 (TLS)에 등록하지 못했습니다. SIP 타이머 F가 만료되면 전화기는 시간 T2 (T2=T1+SIP Timer F)에 2.2.2.2 (UDP)에 등록합니다. 현재 연결은 UDP를 통해 2.2.2.2에 있습니다.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS          DOWN        T1 (Down time)
2nd            2.2.2.2            UDP          UP
3rd            3.3.3.3            TCP          UP
```

전화기에 다음과 같은 구성이 있습니다.

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

여기서 *n*은 내선 번호입니다.

전화기가 시간 T2 (T2=(3600-16)*78%)에 등록을 새로 고칩니다. 전화기가 주소 목록을 확인하여 IP 주소의 가용성 및 다운 시간을 확인합니다. T2-T1 > = 60인 경우 실패한 서버 1.1.1.1이 다시 시작되고 목록이 다음으로 업데이트됩니다. 전화기가 1.1.1.1에 SIP 메시지를 보냅니다.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS           UP
2nd            2.2.2.2            UDP           UP
3rd            3.3.3.3            TCP           UP
```

TCP 또는 **TLS** 연결에서 장애 복구

TCP 또는 TLS 연결에서 장애 복구는 매개 변수 프록시 폴백 간격에 의해 트리거됩니다. 다음 예에서는 전화기가 T1에 1.1.1.1 (UDP)에 등록하지 못했으므로 2.2.2.2 (TCP)에 등록합니다. 현재 연결은 TCP를 통해 2.2.2.2에 있습니다.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            UDP          DOWN        T1 (Down time)
2nd            2.2.2.2            TCP          UP
3rd            3.3.3.3            TLS          UP
```

전화기에 다음과 같은 구성이 있습니다.

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

여기서 *n*은 내선 번호입니다.

프록시 폴백 간격(60초)은 T1에서 카운트다운됩니다. 전화기가 T1+60일 때 프록시 장애 복구를 트리거합니다. 이 예에서 프록시 폴백 간격을 0으로 설정하는 경우 전화기는 2.2.2.2에 연결을 유지합니다.

이중 등록

전화기는 항상 기본(또는 기본 아웃바운드) 및 대체(또는 대체 아웃바운드) 프록시로 등록합니다. 등록 이후에 전화기는 우선 기본 프록시를 통해 Invite 및 Non-Invite SIP 메시지를 전송합니다. 새 INVITE에 대한 시간 초과 이후에 기본 프록시로부터 응답이 없는 경우 전화기는 대체 프록시로의 연결을 시도합니다. 전화기가 기본 프록시로 등록하지 못하는 경우 기본 프록시로 시도하지 않고 대체 프록시로 INVITE를 전송합니다.

참고 MPP 전화기는 UDP 연결을 통해서만 이중 등록을 지원합니다.

회선당 방식으로 이중 등록이 지원됩니다. 웹 사용자 인터페이스 및 원격 프로비저닝을 통해 3개의 추가 매개 변수를 구성할 수 있습니다.

- 대체 프록시—기본값는 공백입니다.
- 대체 아웃바운드 프록시—기본값는 공백입니다.
- 이중 등록—기본값는 아니요(꺼짐)입니다.

매개 변수를 구성한 이후 전화기를 재부팅하여 기능을 적용합니다.

참고 기본 프록시(또는 기본 아웃바운드 프록시) 및 대체 프록시(또는 대체 아웃바운드 프록시)에 대한 값을 지정하여 기능이 올바르게 작동하도록 합니다.

이중 등록 및 **DNS SRV** 제한 사항

- 이중 등록이 활성화된 경우 DNS SRV 프록시 폴백 또는 복구가 비활성화되어야 합니다.
- 기타 폴백 또는 복구 매커니즘과 함께 이중 등록을 사용하지 마십시오. 예: Broadsoft 메커니즘.
- 기능 요청에 대한 복구 매커니즘은 없습니다. 그러나 관리자는 기본 및 대체 프록시에 대한 등록 상태 즉시 업데이트 재등록 시간을 조정할 수 있습니다.

이중 등록 및 대체 프록시

이중 등록 매개 변수가 아니요로 설정된 경우 대체 프록시가 무시됩니다.

RFC3311

Cisco IP 전화기는 RFC 3311, SIP 업데이트 방법을 지원합니다.

SIP NOTIFY XML 서비스

Cisco IP 전화기는 SIP NOTIFY XML 서비스 이벤트를 지원합니다. XML 서비스 이벤트와 함께 SIP NOTIFY 메시지 수신 시 메시지에 올바른 자격 증명이 포함되지 않은 경우 전화기는 401 응답과 함께

NOTIFY를 요청합니다. 클라이언트는 IP 전화기의 해당 회선에 대하여 SIP 계정 암호와 함께 MD5 다이제스트를 사용하여 올바른 자격 증명을 제공해야 합니다.

메시지 본문에는 XML 이벤트 메시지가 포함될 수 있습니다. 예:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

인증:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

Cisco Discovery Protocol

CDP (Cisco 탐색 프로토콜)는 협상 기반으로 Cisco IP 전화기가 위치하는 가상 LAN(VLAN)을 결정합니다. Cisco 스위치를 사용하는 경우 CDP를 사용할 수 있고 기본적으로 활성화됩니다. CDP의 특성은 다음과 같습니다.

- 인접 장치의 프로토콜 주소를 획득하고 해당 장치의 플랫폼을 검색합니다.
- 라우터가 사용하는 인터페이스에 대한 정보를 표시합니다.
- 미디어 및 프로토콜 독립적입니다.

CDP 없이 VLAN을 사용하는 경우 Cisco IP 전화기에 대한 VLAN ID를 입력해야 합니다.

LLDP-MED

Cisco IP 전화기는 레이어 2 자동 검색 방식을 사용하는 Cisco 또는 기타 타사 네트워크 연결 장치에 대하여 미디어 엔드포인트 장치를 위한 링크 레이어 검색 프로토콜(LLDP-ME)을 지원합니다. LLDP-MED에 대한 구현은 2005년 5월 IEEE 802.1AB (LLDP) 사양 및 2006년 4월 ANSI TIA-1057에 따라 완료되었습니다.

Cisco IP 전화기는 미디어 엔드포인트 검색 참조 모델 및 정의(ANSI TIA-1057 섹션 6)에 따라 네트워크 연결 장치로의 직접 LLDP-MED 링크가 있는 LLDP-MED 미디어 엔드포인트 클래스 III 장치로 작동합니다.

Cisco IP 전화기는 LLDP-MED 미디어 엔드포인트 장치 클래스로 다음의 제한적인 유형-길이-값(TLV)만 지원합니다.

- 섀시 ID TLV
- 포트 ID TLV
- TTL(Time to live) TLV
- 포트 설명 TLV

- 시스템 이름 TLV
- 시스템 기능 TLV
- IEEE 802.3 MAC/PHY 구성/상태 TLV(유선 네트워크 전용)
- LLDP-MED 기능 TLV
- LLDP-MED 네트워크 정책 TLV (애플리케이션 유형=음성 전용인 경우)
- MDI TLV를 통한 LLDP-MED 확장 전원 TLV(유선 네트워크 전용)
- LLDP-MED 펌웨어 개정 TLV
- LLDPDU TLV의 끝

해당하는 경우 발신 LLDPDU에는 모든 이전 TLV가 포함됩니다. 수신 LLDPDU의 경우 다음 TLV가 누락된 경우 LLDPDU가 삭제됩니다. 모든 기타 TLV는 유효성이 검사되지 않고 무시됩니다.

- 섀시 ID TLV
- 포트 ID TLV
- TTL(Time to live) TLV
- LLDP-MED 기능 TLV
- LLDP-MED 네트워크 정책 TLV (애플리케이션 유형=음성 전용인 경우)
- LLDPDU TLV의 끝

해당하는 경우 Cisco IP 전화기는 종료 LLDPDU를 전송합니다. LLDPDU 프레임에는 다음 TLV가 포함됩니다.

- 섀시 ID TLV
- 포트 ID TLV
- TTL(Time to live) TLV
- LLDPDU TLV의 끝

Cisco IP 전화기에서의 LLDP-MED 구현에는 몇 가지 제한 사항이 있습니다.

- 인접 정보의 저장 및 검색은 지원되지 않습니다.
- SNMP 및 해당 MIB는 지원되지 않습니다.
- 통계 카운터 레코딩 및 검색은 지원되지 않습니다.
- 모든 TLV에 대한 전체 유효성 검사는 수행되지 않고 전화기에 적용되지 않는 TLV는 무시됩니다.
- 표준에 명시된 대로 프로토콜 상태 시스템은 참조용으로만 사용됩니다.

섀시 ID TLV

발신 LLDPDU의 경우 TLV는 하위=5(네트워크 주소)를 지원합니다. IP 주소를 아는 경우 섀시 ID의 값은 INAN 주소 패밀리의 옥텟 + 음성 통신에 사용되는 IPv4 주소에 대한 옥텟 문자열입니다. IP 주소를 모르는 경우 섀시 ID의 값은 0.0.0.0입니다. 지원되는 유일한 INAN 주소 패밀리는 IPv4입니다. 현재, 섀시 ID에는 IPv6 주소가 지원되지 않습니다.

수신 LLDPDU의 경우 섀시 ID는 MSAP 식별자를 구성하는 불투명 값으로 처리됩니다. 값은 하위에 대한 유효성이 확인되지 않습니다.

섀시 ID TLV는 첫 번째 TLV로 필수입니다. 섀시 ID는 발신 및 수신 LLDPDU에 대해서만 허용됩니다.

포트 ID TLV

발신 LLDPDU의 경우 TLV는 하위=3(MAC 주소)를 지원합니다. 이더넷 포트에 대한 6 옥텟 MAC 주소는 포트 ID의 값으로 사용됩니다.

수신 LLDPDU의 경우 포트 ID TLV는 MSAP 식별자를 구성하는 불투명 값으로 처리됩니다. 값은 하위에 대한 유효성이 확인되지 않습니다.

포트 ID TLV는 두 번째 TLV로 필수입니다. 1개의 포트 ID TLV만 발신 및 수신 LLDPDU에 대해 허용됩니다.

TTL(Time to Live) TLV

발신 LLDPDU의 경우 TTL 값은 180초입니다. 이 값은 표준 권장 시간인 120초와 다릅니다. 종료 LLDPDU의 경우 TTL 값은 항상 0입니다.

세 번째 TLV의 경우 TTL TLV는 필수입니다. 발신 및 착신 LLDPDU에 대하여 1개의 TTL TLV만 허용됩니다.

LLDPDU TLV의 끝

값은 2옥텟으로 모두 0입니다. 이 TLV는 필수이며 발신 및 착신 LLDPDU에 대하여 하나만 허용됩니다.

포트 설명 TLV

발신 LLDPDU의 경우 포트 설명 TLV에서 포트 설명에 대한 값은 CDP의 "포트 ID TLV"와 동일합니다. 수신 LLDPDU의 경우 포트 설명 TLV는 무시되고 유효성이 확인되지 않습니다. 발신 및 수신 LLDPDU에는 1개의 포트 설명 TLV만 허용됩니다.

시스템 이름 TLV

Cisco IP 전화기의 경우 값은 SEP+MAC 주소입니다.

예**:** SEPAC44F211B1D0

착신 LLDPDU인 시스템 이름 TLV는 무시되고 유효성이 확인 되지 않습니다. 발신 및 착신 LLDPDU에 대한 1개의 시스템 이름 TLV만 허용됩니다.

시스템 기능 **TLV**

시스템 기능 TLV에서 발신 LLDPDU의 경우 2 옥텟 시스템 기능 필드에 대한 비트 값은 비트 2(브리지)로 설정되고 PC 포트가 있는 전화기의 경우 비트 5(전화기)로 설정되어야 합니다. 전화기에 PC 포트가 없는 경우에는 비트 5만 설정되어야 합니다. 동일한 시스템 기능 값이 활성화된 기능 필드에 설정되어야 합니다.

수신 LLDPDU의 경우 시스템 기능 TLV은 무시됩니다. TLV는 MED 장치 유형에 대한 의미 체계 유효성 검사가 수행되지 않습니다.

시스템 기능 TLV는 발신 LLDPDU의 경우 필수입니다. 1개의 시스템 기능 TLV만 허용됩니다.

관리 주소 **TLV**

TLV는 로컬 LLDP 에이전트와 연결된 주소(상위 레이어 엔티티에 도달하기 위해 사용될 수 있음)를 식별하여 네트워크 관리에서의 검색을 지원합니다. TLV를 사용하면 둘 중 하나 또는 둘 다 알고 있는 경우 이 관리 주소와 연결된 시스템 인터페이스 번호 및 개체 식별자(OID) 모두를 포함할 수 있습니다.

- TLV 정보 문자열 길이—이 필드에는 TLV 정보 문자열의 모든 필드 길이(옥텟)를 포함합니다.
- 관리 주소 문자열 길이—이 필드에는 관리 주소 하위 유형 + 관리 주소 필드의 길이(옥텟)가 포함됩니다.

시스템 설명 **TLV**

TLV를 사용하면 네트워크 관리가 시스템 설명을 알릴 수 있습니다.

- TLV 정보 문자열 길이—이 필드는 시스템 설명의 정확한 길이(옥텟 단위)를 나타냅니다.
- 시스템 설명—이 필드에는 네트워크 엔티티의 텍스트 설명인 영숫자 문자열이 포함됩니다. 시스템 설명에는 시스템 하드웨어 유형, 소프트웨어 운영 체제 및 네트워킹 소프트웨어의 전체 이름 및 버전 ID가 포함됩니다. IETF RFC 3418을 지원하는 구현의 경우 이 필드에 sysDescr 개체를 사용해야 합니다.

IEEE 802.3 MAC/PHY 구성/상태 **TLV**

TLV는 자동 협상을 위한 것이 아니고 문제 해결을 위한 것입니다. 수신 LLDPDU의 경우 TLV가 무시되고 유효성이 검사되지 않습니다. 발신 LLDPDU의 경우 옥텟 값 자동 협상 지원/상태는 다음과 같아야 합니다.

- 비트 0—1로 설정되면 자동 협상 지원 기능이 지원됨을 나타냅니다.

- 비트 1—1로 설정되면 자동 협상 상태가 활성화됨을 나타냅니다.
- 비트 2-7—0으로 설정됩니다.

2옥텟 PMD 자동 협상 알림 기능 필드에 대한 비트 값은 다음과 같이 설정되어야 합니다.

- 비트 13—10BASE-T 반이중 모드
- 비트 14—10BASE-T 전이중 모드
- 비트 11—100BASE-TX 반이중 모드
- 비트 10—100BASE-TX 전이중 모드
- 비트 15—알 수 없음

비트 10, 11, 13 및 14는 설정되어야 합니다.

2 옥텟 운영 MAU 유형에 대한 값이 설정되어 실제 운영 MAU 유형을 반영해야 합니다.

- 16—100BASE-TX 전이중
- 15—100BASE-TX 반이중
- 11—10BASE-T 전이중
- 10—10BASE-T 반이중

예를 들어, 일반적으로 전화기는 100BASE-TX 전이중으로 설정되어야 합니다. 그리고 값 16이 설정되어야 합니다. TLV는 유선 네트워크의 경우 선택 사항이고 무선 네트워크에는 적용되지 않습니다. 전화기는 유선 모드에서만 이 TLV를 전송합니다. 전화기가 자동 협상으로 설정되지 않지만 특정 속도/전이중/반이중으로 설정된 경우 발신 LLDPDU TLV의 경우 옥텟 값 자동 협상 지원/상태를 위한 비트 1은 제거(0)되어야 자동 협상이 비활성화되었음을 나타낼 수 있습니다. 2 옥텟 PMD 자동 협상 통지 기능 필드는 0x8000으로 설정되어야 알 수 없음을 나타냅니다.

LLDP-MED 기능 TLV

발신 LLDPDU의 경우 TLV는 2옥텟 기능 필드용으로 설정된 다음 비트와 함께 장치 유형 3(엔드 포인트 클래스 III)을 가져야 합니다.

비트 위치	기능
0	LLDP-MED 기능
1	네트워크 정책
4	PD MDI를 통해 확장된 전원
5	재고

MED LLDP TLV가 없는 경우, 수신 TLV에 대한 LLDPDU가 삭제됩니다. LLDP-MED 기능 TLV는 필수이며 발신 및 착신 LLDPDU에 대하여 하나만 허용됩니다. LLDP-MED 기능 TLV 이전에 위치하는 경우 기타 모든 LLDP-MED TLV는 무시됩니다.

네트워크 정책 **TLV**

TLV에서 발신 LLDPDU의 경우 VLAN 또는 DSCP가 결정되기 전에 알 수 없는 정책 플래그(U)는 1로 설정됩니다. VLAN 설정 또는 DSCP를 아는 경우 값을 0으로 설정합니다. 정책을 알 수 없는 경우 다른 모든 값을 0으로 설정합니다. VLAN이 결정되거나 사용되기 전에 태그 지정 플래그(T)는 0으로 설정됩니다. 태그 지정 VLAN(VLAN ID > 1)이 전화기에 사용되는 경우 태그 지정 플래그(T)는 1로 설정됩니다. 예약됨(X)는 항상 0으로 설정됩니다. VLAN이 사용되는 경우 해당 VLAN ID 및 L2 우선 순위는 그에 따라 설정됩니다. VLAN ID 유효한 값 범위는 1~4094입니다. 그러나 VLAN ID=1은 사용되지 않습니다(제한 사항). DSCP가 사용되는 경우 0~63의 값 범위가 그에 따라 설정됩니다.

TLV에서 수신 LLDPDU의 경우 다른 애플리케이션 유형에 대한 다중 네트워크 정책 TLV가 허용됩니다.

MDI TLV를 통한 **LLDP-MED** 확장 전원

발신 LLDPDU에 대한 TLV에서 전원 유형에 대한 이진 값은 “0 1”로 설정되어 전화기의 전원 유형이 PD 장치임을 나타냅니다. 전화기에 대한 전원 공급장치는 이진 값이 "1 1"인 "PSE 및 로컬"로 설정됩니다. 전원 우선 순위는 이진값 "0 0 0 0"으로 설정되어 전원값이 최대 전원값으로 설정된 경우 알 수 없는 우선 순위임을 나타냅니다. Cisco IP 전화기에 대한 전원값은 12900mW입니다.

수신 LLDPDU의 경우 TLV가 무시되고 유효성이 검사되지 않습니다. 발신 및 수신 LLDPDU에서는 1개의 TLV만 허용됩니다. 전화기는 유선 네트워크에만 TLV를 전송합니다.

LLDP-MED 표준은 원래 이더넷 환경에서 초안이 작성되었습니다. 무선 네트워크에서의 LLDP-MED에 대한 논의가 현재 진행 중입니다. ANSI-TIA 1057, 부록 C의 C.3 VoWLAN에 적용 가능한 TLV(테이블 24)를 참조하세요. 이 경우에는 무선 네트워크의 컨텍스트에서 TLV를 적용할 수 없는 것이 좋습니다. 이 TLV는 PoE 및 이더넷 환경에서 사용하는 것을 목적으로 합니다. 추가된 경우 TLV는 스위치에서의 전원 정책 조정 또는 네트워크 관리를 위한 값을 제공하지 않습니다.

LLDP-MED 재고 관리 **TLV**

이 TLV는 장치 클래스 III의 경우 선택 사항입니다. 발신 LLDPDU의 경우 펌웨어 개정 TLV만 지원됩니다. 펌웨어 개정의 값은 전화기의 펌웨어 버전입니다. 수신 LLDPDU의 경우 TLV가 무시되고 유효성이 검사되지 않습니다. 발신 및 수신 LLDPDU에 대하여 1개의 펌웨어 개정 TLV만 허용됩니다.

최종 네트워크 정책 해결 및 QoS

특수 VLAN

VLAN=0, VLAN=1 및 VLAN=4095는 태그가 지정되지 않은 VLAN과 동일한 방식으로 취급됩니다. VLAN은 태그가 지정되지 않으므로 서비스 클래스(CoS)가 적용되지 않습니다.

SIP 모드에 대한 기본 QoS

CDP 또는 LLDP MED에서 네트워크 정책이 없는 경우 기본 네트워크 정책이 사용됩니다. CoS는 특정 내선 번호에 대한 구성을 기준으로 합니다. 수동 VLAN이 활성화되고 수동 VLAN ID가 0, 1 또는 4095과 같지 않은 경우에만 해당됩니다. ToS(서비스 유형)는 특정 내선 번호에 대한 설정을 기준으로 합니다.

CDP에 대한 QoS 해상도

CDP에서 유효한 네트워크 정책이 있는 경우:

- VLAN = 0, 1 또는 4095인 경우 VLAN 설정되지 않거나 VLAN이 태깅되지 않습니다. CoS를 적용할 수 없지만 DSCP는 적용할 수 있습니다. 이전 설명과 같이 ToS는 기본값에 기반합니다.
- VLAN > 1이고 VLAN < 4095인 경우, VLAN은 그에 따라 설정됩니다. CoS 및 ToS는 이전 설명과 같이 기본값에 기반합니다. DSCP가 적용됩니다.
- 전화기가 재부팅되고 빠른 시작 순서가 다시 시작됩니다.

LLDP-MED에 대한 QoS 해상도

CoS가 적용되고 CoS=0인 경우, 이전의 설명과 같이 특정 내선 번호에는 기본값가 사용됩니다. 그러나 발신 LLDPDU의 TLV에 대한 L2 우선 순위에 표시되는 값은 내선 번호 1에 사용되는 값을 기반으로 합니다. CoS가 적용되고 CoS!=0인 경우 모든 내선 번호에서 CoS가 사용됩니다.

DSCP(ToS에 매핑)가 적용되고 DSCP=0인 경우, 이전의 설명과 같이 특정 내선 번호에는 기본값가 사용됩니다. 그러나 발신 LLDPDU의 TLV에 대한 DSCP에 표시되는 값은 내선 번호 1에 사용되는 값을 기반으로 합니다. DSCP가 적용되고 DSCP!=0인 경우, 모든 내선 번호에서 DSCP가 사용됩니다.

VLAN > 1이고 VLAN < 4095인 경우, VLAN은 그에 따라 설정됩니다. CoS 및 ToS는 이전 설명과 같이 기본값에 기반합니다. DSCP가 적용됩니다.

LLDP-MED PDU에서 음성 애플리케이션에 대한 유효한 네트워크 정책이 있는 경우 및 태깅된 플래그가 설정된 경우에는 VLAN, L2 우선 순위(CoS) 및 DSCP(ToS에 매핑)가 모두 적용됩니다.

LLDP-MED PDU에서 음성 애플리케이션에 대한 유효한 네트워크 정책이 있는 경우 및 태깅된 플래그가 설정되지 않은 경우에는 DSCP(ToS에 매핑)만 적용됩니다.

Cisco IP 전화기가 재부팅되고 빠른 시작 순서가 다시 시작됩니다.

CDP와 동시 사용

CDP 및 LLDP-MED가 모두 활성화된 경우 VLAN에 대한 네트워크 정책은 검색 모드 중 하나를 사용하여 마지막으로 설정되거나 변경된 정책을 결정합니다. LLDP-MED 및 CDP가 모두 활성화된 경우 시작하는 동안 전화기는 CDP 및 LLDP-MED PDU를 전송합니다.

CDP 및 LLDP-MED 모드를 위한 네트워크 연결 장치의 구성 및 동작에 일관성이 없는 경우 다른 VLAN으로의 전환으로 인해 전화기 재부팅 동작이 반복될 수 있습니다.

CDP 및 LLDP-MED로 VLAN이 설정되지 않은 경우 수동으로 구성된 VLAN ID가 사용됩니다. VLAN ID가 수동으로 구성되지 않은 경우 VLAN이 지원되지 않습니다. DSCP가 사용되는 해당되는 경우 네트워크 정책이 LLDP-MED를 결정합니다.

LLDP-MED 및 다중 네트워크 장치

네트워크 정책에 동일한 애플리케이션 유형이 사용되지만 다중 네트워크 연결 장치에서 다른 레이어 2 또는 레이어 3 QoS 네트워크 정책이 수신되는 경우 마지막으로 유효한 네트워크 정책이 적용됩니다. 일관적인 고정 네트워크 정책을 사용하려면 다중 네트워크 연결 장치가 동일 애플리케이션 유형에 서로 다른 네트워크 정책을 전송하지 않아야 합니다.