

Cisco 1711 및 1712 Security Access Router

Cisco® 1711 및 1712 Security Access Router는 소규모 기업 지사와 중소 규모 기업의 안전하고 신뢰할 수 있는 인터넷 및 기업 네트워크 연결을 제공하는 데 최적의 라우터입니다. 이 라우터는 내장된 고속 이더넷 LAN 스위칭, 고속 이더넷 WAN 또는 DSL 광대역 모뎀 연결을 통해 올인원(all-in-one) 보안 및 라우팅 솔루션을 제공하며, 중요한 비즈니스 애플리케이션의 고가용성을 보장하기 위해 ISDN 또는 아날로그 모뎀 백업 인터페이스를 제공합니다. 또한, Cisco 1711 및 1712 라우터는 네트워크를 보호하고 인터넷을 통해 데이터를 안전하게 전송하기 위해 통합된 네트워크 보안 서비스를 지원합니다.

중소 규모 비즈니스에 배치된 Cisco 1711 및 1712 라우터는 인터넷 및 다른 원격 지사에 대한 액세스를 제공할 뿐만 아니라, Cisco IOS® Software 보안 기능을 통해 비즈니스에 필수적인 데이터의 보안을 유지하고 보호합니다. 소규모 기업 지사에 배치된 Cisco 1711 및 1712 라우터는 기업 본사나 다른 지사에 안전하고 신뢰할 수 있는 연결을 제공함으로써 기업 인트라넷 액세스 권한을 직원에게 제공합니다.

Cisco 1711 및 1712 라우터는 라우터, 고속 이더넷 스위치, 방화벽, VPN(Virtual Private Network), IDS(Intrusion Detection System) 및 리턴던시형 WAN 인터페이스와 같이 일반적으로 별도의 장치를 통해서 제공되는 여러 서비스를 단일 장

치를 통해 제공하므로 기업에서는 비용을 줄일 수 있습니다. Cisco IOS Software에서 제공하는 유연성을 통해 업계에서 가장 강력하고 확장성이 뛰어난 다양한 기능의 인터넷워킹 소프트웨어 지원을 제공하며, 이를 위해 인터넷과 사실 WAN용으로 승인을 받은 표준 네트워킹 소프트웨어를 사용합니다.

통합 LAN 스위칭

Cisco 1711 및 1712 라우터의 4포트 10/100BASE-TX 고속 이더넷 스위치를 통해 비즈니스가 단일 장치에서 LAN 및 WAN 구성을 지원하고 관리할 수 있습니다. Spanning Tree Protocol 802.1D를 지원하는 스위치 인터페이스를 사용하여 최대 4개의 물리적 LAN이나 최대 16개의 IEEE 802.1Q 가상 LAN(VLAN)에 연결할 수 있습니다.

또한 Cisco IOS Software에 통합된 보안 기능을 사용하여 회사 인트라넷 내에 DMZ(demilitarized zone)를 만들 수 있습니다(그림 2). 이를 통해 비즈니스의 보안을 유지할 수 있으며, 외부의 위협으로부터 네트워크를 보호하고 고객이 공용 웹 및 FTP 서버에 액세스할 수 있도록 합니다.

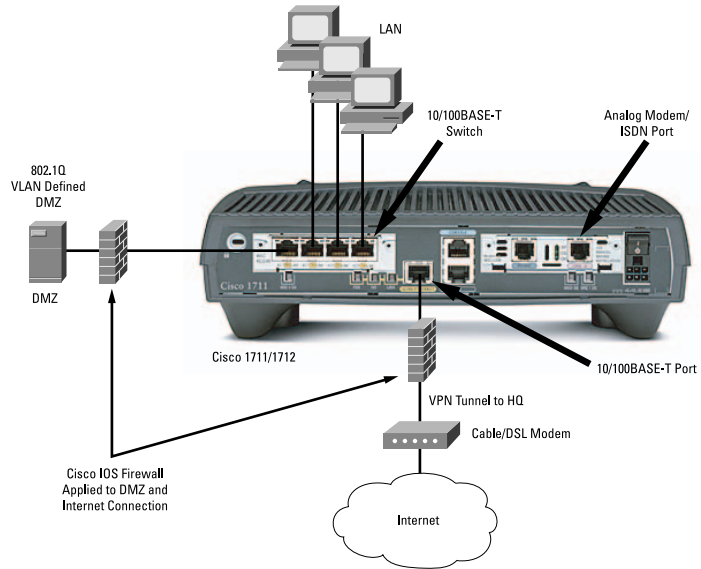
그림 1:
Cisco 1711 또는 1712 라우터





그림 2:

Cisco IOS Firewall을 사용하여 Cisco 1711 및 1712의 고속 이더넷 스위치 포트 상에 DMZ를 만들 수 있습니다.

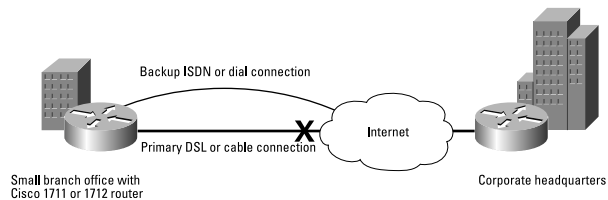


고가용성

Cisco 1712 Router의 ISDN 포트와 Cisco 1711 Router의 아날로그 모뎀 포트는 기본 WAN 연결이 끊어지는 경우에 대비하여 인터넷과 기업 네트워크에 대한 안정적인 액세스를 제공하기 위해 리던던시형 백업 WAN 연결을 제공합니다(그림 3). 또한 Cisco IOS Software를 사용하여 Cisco 1711 및 1712 라우터가 WAN 연결 끊김을 자동으로 감지하고 백업 연결을 통해 연결을 다시 설정할 수 있습니다. Cisco IOS Software는 업계에서 입증된 소프트웨어이며, 안정적인 비즈니스 액세스를 위한 표준으로 자리잡고 있습니다. 이 소프트웨어를 통해 비즈니스는 WAN 연결 중단으로 인해 발생하는 생산성 손실을 막을 수 있습니다.

그림 3:

기본 광대역 연결이 끊어지는 경우 Cisco 1711 Router의 아날로그 모뎀 포트나 Cisco 1712 Router의 ISDN 포트가 백업 WAN 연결로 동작합니다.





통합 네트워크 보안

Cisco 1711 및 1712 라우터는 조직이 생산성을 향상시키고 비용을 절감할 수 있도록 통합된 네트워크 보안 솔루션을 제공합니다.

표준 통합 보안 서비스에는 사이트간 VPN에 사용되는 하드웨어 가속 IP 보안(IPSec) 3DES(Triple Data Encryption Standard) 암호화 및 상태 보존형 검사 방화벽과 네트워크 보호를 위한 Cisco IDS가 있습니다. 이러한 기능은 인터넷을 통해 안전한 연결을 제공하여 지리적으로 분산된 지사, 비즈니스 파트너 및 원격 사용자를 연결해줄 뿐만 아니라 사설 네트워크와 동일한 보안, 트래픽 우선 순위 부여, 관리 및 안정성을 제공합니다.

VPN

기업에서는 VPN을 사용하여 공용 네트워크를 통해 지사, 이동 작업자 및 비즈니스 파트너에 안전하게 연결할 수 있으므로 사설 회선에 비해 상당한 비용이 절감됩니다. 기업에서는 인터넷의 광범위한 공유 커뮤니케이션 인프라나 서비스 제공업체의 공유 백본을 활용함으로써 기존 사설 네트워크에 소요되던 서비스 비용을 절감할 수 있습니다.

Cisco 1711 및 1712 라우터는 하드웨어 지원 VPN 기능을 제공하며 현재 가장 강력한 암호화된 3DES를 사용하여 15 Mbps 속도로 데이터를 암호화합니다. Cisco IOS Software에서는 AES(Advanced Encryption Standard)도 지원합니다. Cisco 1711 및 1712 라우터는 고성능 VPN 암호화 및 터널링 기술을 사용하여 기업 네트워크에 연결되는 안전한 터널을 인터넷 상에 구성할 수 있습니다. 필요한 경우에만 가상 네트워크가 연결되므로, 임대 회선을 사용하지 않은 시간에 대해서는 더 이상 값비싼 비용을 지불하지 않아도 됩니다. 안전한 글로벌 커뮤니케이션 웹 상에서 최대 100개의 동시 터널이나 사이트를 지원할 수 있도록 Cisco 1711 또는 1712 라우터를 사용하여 VPN을 확장할 수 있습니다.

방화벽 및 IDS

항시 인터넷에 연결되어 있는 광대역 연결의 경우 원하지 않는 침입이나 악의적인 인터넷 공격으로부터 내부 네트워크를 보호하는 것이 매우 중요합니다. 통합된 상태 보존형 검사 방화벽은 내부 사용자의 안전한 인터넷 액세스를 가능하게 하며 서비스 거부(DoS) 공격이나 기타 무단 액세스로부터 내부 네트워크를 보호해 줍니다.

Cisco 1711 및 1712 라우터는 네트워크의 모든 경계에 강력한 방화벽과 IDS 기능을 통합합니다. 이 라우터는 첨단 보안 기능을 통해 인증 및 암호화와 같은 Cisco IOS Software 보안 솔루션에 뛰어난 유연성을 더해줍니다. 이러한 보안 기능으로는 애플리케이션 기반 상태 필터링, CBAC(Context-Based Access Control), DoS 보호, 사용자 별 동적 인증 및 권한 부여, 네트워크 공격 차단, Java 차단 및 실시간 경보 등이 있습니다.

고급 보안

Cisco 1711 및 1712 라우터에서 지원하는 고급 보안 기능으로는 Cisco Easy VPN Server 및 Cisco Easy VPN Remote, Cisco SDM(Security Device Manager), Cisco AutoSecure 및 방화벽 Websense URL 필터링 등이 있습니다.

Cisco Easy VPN 소프트웨어를 통해 VPN을 간편하게 배치하고 관리할 수 있습니다. 라우터에서 Cisco Easy VPN Server 기능과 함께 하드웨어 암호화 모듈을 사용하여 VPN을 설정할 수 있으며, 이 VPN은 VPN 클라이언트 소프트웨어를 PC에서 실행 중인 원격 작업자에 의해 초기화됩니다. 이 기능을 통해 직원이 정보와 애플리케이션에 언제든지 액세스할 수 있으므로 비즈니스 생산성이 향상됩니다. 또한, 기업 고객은 Easy VPN Remote 기능을 사용하여 보안 정책에 따라 사이트간 VPN을 구성할 수 있으므로 IT 지원 비용이 절감됩니다. 이 보안 정책은 기업의 본사에서 소규모 기업 지사로 전달됩니다.



Cisco IOS AutoSecure 기능을 사용하면 단 한 번의 Cisco IOS Software 명령만으로 네트워크 공격에 이용당할 수 있는 공용 IP 서비스를 사용하지 않도록 지정할 수 있으며, 또한 공격으로부터 네트워크를 보호하도록 도와주는 IP 서비스와 기능을 사용하도록 설정할 수 있습니다. 또한, 이 기능을 통해 라우터의 보안 구성을 단순화하고 라우터 구성을 강화할 수 있습니다.

방화벽 Websense URL 필터링 기능을 통해 Cisco IOS Firewall이 Websense URL 필터링 소프트웨어와 상호 작용할 수 있으며, 보안 정책에 따라 사용자가 특정 웹 사이트에 액세스하지 못하도록 차단할 수 있습니다. Cisco IOS Firewall은 Websense 서버와 함께 사용되어 특정 URL의 허용 또는 거부(차단) 여부를 알아냅니다.

고급 QoS

Cisco QoS 기능은 네트워크의 성능을 극대화하고 애플리케이션 데이터를 구분하여 가장 중요한 애플리케이션에 WAN 회선 사용 우선권을 부여함으로써 기업이 WAN 액세스 비용을 절감하도록 도와줍니다. Cisco 1711 및 1712 라우터에는 RSVP(Resource Reservation Protocol), WFQ(Weighted Fair Queuing) 및 IP Precedence와 같은 고급 QoS 기능이 표준으로 제공됩니다. 성능 향상을 위해 CAR(Committed Access Rate), 정책 라우팅, LLQ(Low-Latency Queuing), GTS(Generic Traffic Shaping), FRTS(Frame Relay Traffic Shaping) 및 RSVP와 같은 기능을 사용하여 WAN 대역폭을 할당할 수 있습니다.

뛰어난 관리

Cisco 1711 및 1712 라우터는 Cisco SDM, CiscoWorks, CiscoView 및 CiscoWorks SNMS(Small Network Management Solution)와 같은 뛰어난 관리 애플리케이션과 설치가 용이한 툴을 제공합니다.

Cisco SDM은 직관적인 웹 기반의 장치 관리 툴로 Cisco IOS Software 액세스 라우터에 포함되어 있습니다. SDM은 고객이 Cisco IOS Software CLI에 대해 모르더라도 스마트 마법사를 사용하여 시스코 액세스 라우터를 쉽고 빠르게 구성하고 모니터링할 수 있도록 도와주므로 라우터와 보안 구성이 단순화됩니다.

Cisco SDM은 Cisco 1711 및 1712 라우터에 방화벽, VPN 및 NAT(Network Address Translation)와 같은 보안 서비스를 신속하게 구축할 수 있는 사용이 용이한 새로운 기능을 제공합니다. Cisco SDM의 인텔리전트 마법사는 사용자가 LAN/WAN 인터페이스, 방화벽 및 VPN을 구성하는 방법을 단계별로 안내합니다. 또한, Cisco SDM 마법사는 잘못된 보안 구성을 자동으로 감지한 후 해결 방법을 제시할 수 있습니다. 예를 들어, WAN 인터페이스가 DHCP 어드레스되는 경우 방화벽을 통해 DHCP(Dynamic Host Control Protocol)를 허용할 수 있습니다.

Cisco SDM의 또 다른 새로운 기능은 보안 감사 기능입니다(그림 4). 이 기능을 통해 사용자가 기존 라우터 구성에 대한 보안 감사 보고서를 만든 후 ICSA Labs 및 Cisco TAC(Technical Assistance Center)에서 권장하는 구성에 따라 단 한번의 클릭으로 라우터 구성을 고정시킬 수 있습니다. Cisco SDM은 Cisco IOS Software CLI에 익숙하지 않은 사용자의 생산성을 인텔리전트 마법사를 통해 높이도록 설계되었습니다. 또한, Cisco SDM은 숙련된 Cisco IOS Software 사용자가 마법사에서 만들어진 표준 방화벽/VPN 구성을 사이트에 보다 적합한 고유의 구성으로 조정할 수 있도록 설계되었습니다. Cisco SDM에는 숙련된 사용자가 Cisco SDM에서 생성된 모든 구성을 Cisco IOS Software CLI 형식으로 볼 수 있는 Cisco IOS Software CLI 미리 보기 모드가 있습니다.

업계 최고의 웹 기반 네트워크 관리 제품군인 CiscoWorks는 Cisco 1711 및 1712 라우터를 원격으로 구성, 관리, 모니터링 및 문제 해결 기능을 제공합니다. 또한 성능 병목 현상과 장기적인 성능 추세를 신속하게 식별함으로써 네트워크 동작에 대한 가시성을 향상시켜줍니다. CiscoWorks는 고가의 필수적인 네트워크 WAN 연결에서 대역폭과 사용량을 최적화해 주는 정교한 구성 툴을 제공합니다.



CiscoWorks SNMS는 웹 기반의 광범위한 네트워크 관리 솔루션입니다. 이 솔루션은 최대 20대의 시스코 인터넷 워킹 제품(스위치, 라우터, 허브 및 액세스 서버)이 포함된 중소 규모 비즈니스 네트워크와 작업 그룹의 관리를 단순화 해 주는 강력한 기능의 모니터링, 구성 및 관리 툴을 제공합니다.

네트워크 보안을 위한 SAFE Blueprint의 중요한 일부인 CiscoWorks VMS(VPN/Security Management Solution)에는 엔터프라이즈 VPN, 방화벽, 네트워크 및 호스트 기반 IDS의 구성, 모니터링 및 문제 해결을 위한 웹 기반 툴이 통합되어 있습니다. CiscoWorks VMS는 업계에서 가장 강력하고 확장성이 뛰어난 구조와 기능 세트를 제공하여 소규모 및 대규모 VPN과 보안 배치의 요구사항을 충족시킵니다.

ISDN – ADSL 마이그레이션

Cisco 1712 Router는 경제적인 비용으로 ISDN에서 ADSL 서비스로 마이그레이션할 수 있는 방법을 제공합니다. ISDN이 WAN 액세스 기술로 널리 사용되고 있는 여러 국가에서 ADSL이 점차적으로 WAN 액세스를 위해 사용되고 있습니다. Cisco 1712 Router를 통해 고객이 처음에 ISDN 액세스를 배치할 수 있으며, ADSL 서비스를 사용할 수 있게 되면 라우터를 새로 구입하지 않고도 ADSL로 마이그레이션할 수 있습니다.

표 1 기능 및 혜택

기능	혜택
통합 스위칭	
4개의 10/100BASE-TX 이더넷 포트	<ul style="list-style-type: none"> 단일 장치에서 LAN/WAN 구성을 지원하고 관리할 수 있습니다.
IEEE 802.1Q Inter-VLAN 라우팅 (16개의 VLAN 지원)	<ul style="list-style-type: none"> 회사 LAN의 분할을 허용합니다. DMZ 지원을 통해 네트워크 보안을 향상시킵니다. 브로드캐스트 트래픽 제어를 통해 네트워크 성능을 향상시킵니다.
Spanning Tree Protocol 802.1D	<ul style="list-style-type: none"> 네트워크에서 불필요한 루프를 제거함과 동시에 리던던시형 경로를 제공합니다.
고가용성	
예비 ISDN S/T 포트(Cisco1712에만 해당) 또는 아날로그 모뎀 포트(Cisco 1711에만 해당)	<ul style="list-style-type: none"> 안정적인 액세스를 위해 리던던시형 WAN 연결을 제공함으로써 인터넷 액세스의 가용성과 기업 사이트에 대한 연결을 보장합니다.
OSPF(Open Shortest Path First)와 같은 동적 라우팅 프로토콜을 통한 DDR (Dial-on-Demand Routing)	<ul style="list-style-type: none"> 기본 연결이 끊어지는 경우 WAN 연결을 자동으로 복원합니다.
이중 बैं크 플래시 메모리	<ul style="list-style-type: none"> Cisco IOS Software의 백업 복사본을 플래시 메모리에 저장합니다.
HSRP(Hot Standby Router Protocol)	<ul style="list-style-type: none"> 업스트림 연결은 끊어졌지만 HSRP 장치는 아직 작동 중인 경우 예비 HSRP 장치로 연결을 다시 복원합니다.
통합 보안	
Cisco Easy VPN Server 및 Easy VPN Remote	<ul style="list-style-type: none"> 자동 IPsec 터널 초기화를 통해 VPN 연결을 쉽게 배치하고 간편하게 유지 관리합니다. Cisco 1711 또는 1712 라우터에서 원격 클라이언트 또는 기업의 Cisco VPN 집중 장치나 서버에서 Cisco 1711 또는 1712 라우터로 보안 정책을 전달합니다.
하드웨어 가속 IPsec 3DES 암호화	<ul style="list-style-type: none"> 광대역 연결을 위해 IPsec VPN 암호화를 제공합니다. 최대 100개의 동시 터널을 위해 IKE(Internet Key Exchange) 및 IPsec VPN 표준을 지원합니다.
PKI(Public-Key Infrastructure) 지원	<ul style="list-style-type: none"> 장치 인증 및 키 관리를 제공합니다. IKE, X.509v3 디지털 인증서, Verisign 및 Entrust와 같은 인증 기관(CA)을 통한 CEP(Certificate Enrollment Protocol) 지원을 포함합니다.



표 1 기능 및 혜택(계속)

기능	혜택
AES	<ul style="list-style-type: none"> DES 이상의 보안을 제공합니다. 최대 256비트의 보다 길어진 키 크기를 제공합니다.
상태 보존형 검사 방화벽	<ul style="list-style-type: none"> 네트워크 경계의 모든 트래픽에 대한 안전한 동적 액세스 제어(상태 검사)를 내부 사용자에게 제공합니다. DoS 공격으로부터 라우터 리소스를 보호합니다. CBAC를 제공합니다.
IDS	<ul style="list-style-type: none"> DoS 공격과 무단 네트워크 액세스를 감지하여 차단합니다. 올바른 조치를 취하도록 알려줍니다. 100개의 IDS 서명을 모니터링합니다.
Cisco AutoSecure	<ul style="list-style-type: none"> 사용자가 모든 Cisco IOS Software CLI 기능에 대해 자세히 모르더라도 네트워크를 신속하게 보호할 수 있습니다. 단일 CLI를 사용하여 보안 기능을 잠글 수 있으므로 라우터의 보안 구성이 단순해집니다.
인증, 권한 부여 및 계정 (AAA: Authentication, Authorization, Accounting)	<ul style="list-style-type: none"> HTTP, 텔넷 및 FTP 프로토콜을 인증합니다. RADIUS, TACACS+ 및 로컬 인증을 지원합니다. 네트워크 서비스에 대한 사용자 액세스를 인증합니다. 사용자 네트워크 액세스를 추적합니다.
방화벽 Websense URL 필터링	<ul style="list-style-type: none"> 지정된 보안 정책에 따라 해당 호스트나 사용자에게 대해 웹 트래픽을 제어할 수 있습니다. 키워드 기반의 필터링을 사용합니다. 이 필터링은 특정 키워드에 따라 적용됩니다. 예를 들어, "dog"라는 키워드가 들어간 모든 URL을 거부하는 정책을 사용자가 구성할 수 있습니다. 맞춤 지정된 필터링을 지원합니다. 이 필터링을 사용하면 맞춤 지정된 URL에 정책을 적용할 수 있습니다.
압축	
IPSec 소프트웨어 기반 압축	<ul style="list-style-type: none"> 하드웨어 암호화와 함께 소프트웨어 기반 레이어 3 IPPCP(IP Payload Compression Protocol)를 사용할 수 있습니다.
고급 QoS	
IP QoS : LLQ, WRED, CAR, 등급 기반 트래픽 셰이핑, DiffServ(Differentiated Services)	<ul style="list-style-type: none"> 대역폭을 인텔리전트하게 할당함으로써 여러 애플리케이션의 응답 시간을 일관적으로 유지합니다. 애플리케이션을 구분하고 비즈니스에 중요한 애플리케이션에 WAN 회선 사용 우선권을 부여합니다. 각 세션의 우선 순위에 따라 특정 TCP 세션을 차단하여 폭주를 방지합니다.
ATM QoS : per-VC(per-Virtual Circuit) 대기열 및 트래픽 셰이핑을 사용하는 ATM 트래픽 UBR(Unspecified Bit Rate), VBRnrt(Variable Bit Rate/non-real time), VBRrt 및 CBR(Constant Bit Rate)	<ul style="list-style-type: none"> ATM 수준의 셰이핑을 제공하는 적합한 가상 회로를 통해 트래픽을 전송하는 기능과 다른 등급 또는 동일한 등급의 트래픽 회로 사이에 연결이 차단되지 않도록 보장하는 기능을 통해 실시간 트래픽에 QoS를 제공합니다.

제품 사양

그림 4: Cisco 1711 및 1712의 후면





표 2 부품 번호

부품 번호	설명
CISCO1711-VPN/K9	통합 4포트 스위치, WAN용 10/100BASE-TX 및 아날로그 모뎀 백업이 있는 보안 액세스 라우터
CISCO1712-VPN/K9	통합 4포트 스위치, WAN용 10/100BASE-TX 및 ISDN S/T 백업이 있는 보안 액세스 라우터

물리적 인터페이스/포트

10/100BASE-TX 자동 감지 고속 이더넷 스위치형 포트 4개

- RJ-45 잭
- MDI/MDIX Autocrossover
- 전이중/반이중
- IEEE 802.1Q VLAN 라우팅 (16개의 VLAN)
- Spanning Tree Protocol 802.1D

Cisco 1712 Router의 ISDN BRI 포트 1개

- 64 Kbps 및 128 Kbps 속도의 ISDN 전화 접속 및 ISDN DSL (IDSL)
- IDSL, 프레임 릴레이 및 PPP를 통한 캡슐화
- ISDN WAN 포트 기능은 Cisco 1포트 ISDN WAN 인터페이스 카드(WIC-1B-S/T)와 일치합니다.

Cisco 1711 Router의 아날로그 모뎀 포트 1개

- RJ-11 잭
- 최대 56 Kbps의 속도 지원 (V.90)
- 전화 연결을 위한 별도의 RJ-11 잭
- PPP(Point-to-Point Protocol), MLPPP(Multilink PPP) 및 SLIP(Serial Line Internet Protocol)

10/100BASE-TX 고속 이더넷 WAN 포트 1개(RJ-45)

- 자동 속도 감지
- 자동 이중 협상(duplex negotiation)

예비 포트 1개

- EIA/TIA-232 인터페이스가 있는 RJ-45 잭
- 최대 115.2 Kbps의 비동기 직렬 데이터 속도

콘솔 포트 1개

- EIA/TIA-232 인터페이스가 있는 RJ-45 잭
- 최대 115.2 Kbps의 전송/수신 속도(기본 9600 bps, 네트워크 데이터 포트 아님)

성능 요약

- 방화벽 및 IDS 전송량: 20 Mbps
- 168비트 3DES IPSec VPN 전송량: 15 Mbps
- 128비트 AES IPSec VPN 전송량: 4.5 Mbps
- 동시 VPN 피어 수: 100



메모리

플래시 메모리

- 기본: 32 MB
- 최대: 32 MB

DRAM 메모리

- 기본: 64 MB
- 최대: 128 MB

치수 및 중량

- 가로: 11.2 인치 (28.4 cm)
- 높이: 3.1 인치 (7.85 cm)
- 세로: 8.7 인치 (22.1 cm)
- 무게: 2.9 파운드 (1.32 kg)

전원

- AC 입력 전압: 100 ~ 240 VAC
- 주파수: 47 ~ 64 Hz
- AC 입력 전류: 0.5 A
- 전력 소모: 20W (최대)

환경 사양

- 작동 온도: 32° ~ 104°F (0° ~ 40°C)
- 비작동 온도: -4° ~ 149°F (-20° ~ 65°C)
- 상대 습도: 10 ~ 85%, 비응축, 동작 시; 5 ~ 95%, 비응축, 비동작 시

안전

승인

- UL 1950
- CSA 22.2-No. 950
- EN60950
- EN41003
- AUSTEL TS001
- AS/NZS 3260
- ETSI 300-047
- BS 6301 (전원 공급 장치)

EMI

분류

- AS/NRZ 3548 Class A
- FCC Part 15 Class B



- EN60555-2 Class B
- EN55022 Class B
- VCCI Class II
- CISPR-22 Class B

전자파 내성

표준

- 55082-1 Generic Immunity Specification Part 1: Residential and Light Industry
- IEC 1000-4-2 (EN61000-4-2)
- IEC 1000-4-3 (ENV50140)
- IEC 1000-4-4 (EN61000-4-4)
- IEC 1000-4-5 (EN61000-4-5)
- IEC 1000-4-6 (ENV50141)
- IEC 1000-4-11
- IEC 1000-3-2

네트워크 승인

표준

- 미국 - ATIS/ACTA - TIA/EIA/IS - 968(이전의 Part 68), TIA/EIA/IS-883, T1.TRQ.6-2001, TIA/EIA/TSB-129
- 캐나다 - CS-03
- 일본 - JATE
- 호주 - AS/ACIF: S-02, S-043, C-559; ACA TS-002, TS-003, TS-006, TS-016, TS-031
- 뉴질랜드 - PTC107, PTC200, PTC211, PTC270, CTR3
- 유럽 연합 + 스위스 - Directive 1999/5/EC
- 러시아 - CTR2, CTR3, CTR21, ITU-G.992.1, ITU-G991.2
- 벨라루스 - CTR3, CTR21
- 체코 - CTR2, CTR3, CTR21
- 폴란드 - CTR3, PB-TE ITU-G.992.1
- 헝가리 - CTR2, CTR3, CTR21, ITU-G.992.1
- 싱가포르 - IDA: TS-PSTN1, TS-ISDN1, TS-ADSL
- 대만 - PSTN01, IS6100, ID002
- 브라질 - CTR3, CS-03
- 멕시코 - CTR3, CS-03, FCC Part 68
- 남아프리카 공화국 - CTR3

Cisco 1711/1712 라우터를 비롯한 Cisco 1700 Series는 배포되는 국가의 요구사항을 준수합니다. Cisco 1700 Series는 안전, EMI, 전자파 내성 및 네트워크 승인 표준을 준수합니다. 세부 사항은 시스코 리셀러나 고객 관리자를 통해 구할 수 있습니다.

서비스 및 지원

Cisco 1711 및 1712 라우터에 대한 기술 지원 서비스는 Cisco SMARTnet[®]™ 및 Cisco SMARTnet Onsite 서비스 프로그램을 통해 사용할 수 있습니다. Cisco SMARTnet 지원을 통해 운영 직원의 리소스를 늘릴 수 있습니다. 이 지원을 통해 직원이 온라인과 전화를 통해 풍부한 전문 기술에 액세스할 수 있고, 직원이 마음대로 시스템 소프트웨어를 새롭게 고칠 수 있으며, 다양한 종류의 하드웨어 고급 교체 옵션을 사용할 수 있습니다.

Cisco SMARTnet Onsite에서는 현장 엔지니어의 서비스를 추가함으로써 모든 Cisco SMARTnet 서비스를 제공하고 하드웨어 우선 교체 (Advance-Replacement) 기능을 보완합니다. 현장의 경우 부품 교체 작업을 수행할 인력이 모자라거나 아예 구할 수 없기 때문에 이러한

지원을 제공하는 것이 중요합니다.

표 3은 Cisco SMARTnet 지원의 기능과 혜택을 나타냅니다.

표 3 Cisco SMARTnet 기능

Cisco SMARTnet 지원	Cisco SMARTnet Onsite 지원
기능	혜택
연중무휴로 소프트웨어 업데이트 이용	• 문제를 능동적으로 신속하게 해결
기술 저장소에 웹 액세스	• 시스코 전문 기술과 지식을 활용함으로써 총소유 비용을 절감
TAC를 통한 전화 지원	• 네트워크 다운타임 최소화



www.cisco.com/kr

2004-10-28

■ Gold SI파트너	<ul style="list-style-type: none"> • (주)데이타크레프트코리아 02-6256-7000 • (주)콤텍시스템 02-3289-0114 • (주)링네트 02-6675-1216 • (주)LG씨엔에스 02-6363-5000 	<ul style="list-style-type: none"> • (주)인네트 02-3451-5300 • 쌍용정보통신(주) 02-2262-8114 • 한국후지쯔(주) 02-3787-6000 • (주)인성정보 02-3400-7000 	<ul style="list-style-type: none"> • 한국아이비엠(주) 02-3781-7800 • 에스넷시스템(주) 02-3469-2400 • 한국휴렛팩커드(주) 02-2199-0114
■ Silver SI파트너	<ul style="list-style-type: none"> • (주)시스폴 02-6009-6009 • SK씨앤씨(주) 02-2196-7114/8114 	<ul style="list-style-type: none"> • 한국NCR 02-3279-4423 	<ul style="list-style-type: none"> • 포스데이타주식회사 031-779-2114
■ Local 디스트리뷰터	<ul style="list-style-type: none"> • (주)소프트뱅크커머스코리아 02-2187-0176 	<ul style="list-style-type: none"> • (주)아이넷뱅크 02-3400-7490 	<ul style="list-style-type: none"> • (주)SK 네트워크 02-3788-3673
■ IPT 전문파트너	<ul style="list-style-type: none"> • 에스넷시스템(주) 02-3469-2900 • LG기공 02-2630-5280 	<ul style="list-style-type: none"> • (주)인성정보 02-3400-7000 • (주)컴웨어 02-2631-4300 	<ul style="list-style-type: none"> • 크리스넷 1566-3827
■ IP/VC(Video Conferencing)	<ul style="list-style-type: none"> • (주)컴웨어 02-2631-4300 	<ul style="list-style-type: none"> • (주)텔레트론 031-340-7102 	
■ IPCC전문파트너	<ul style="list-style-type: none"> • 한국IBM 02-3781-7114 • (주)인성정보 02-3400-7000 	<ul style="list-style-type: none"> • 한국HP 02-2199-4272 • 삼성네트워크주식회사 02-3415-6754 	<ul style="list-style-type: none"> • LG기공 02-2630-5280
■ WLAN 전문 파트너	<ul style="list-style-type: none"> • (주)에어키 02-584-3717 	<ul style="list-style-type: none"> • (주)텔레트론 02-6245-7600 	
■ Security 전문 파트너	<ul style="list-style-type: none"> • 코코넷 02-6007-0133 • UNNET Systems 02-565-7034 	<ul style="list-style-type: none"> • (주)토탈인터넷서큐리티시스템 051-743-5940 	<ul style="list-style-type: none"> • 나래시스템 02-2190-5533
■ Optical 전문 파트너	<ul style="list-style-type: none"> • (주)LG씨엔에스 02-6363-5000 	<ul style="list-style-type: none"> • 에스넷시스템(주) 02-3469-2900 	<ul style="list-style-type: none"> • 미리넷주식회사 02-2142-2800
■ CN 전문 파트너	<ul style="list-style-type: none"> • 메버릭시스템 02-6283-7425 		
■ Storage 전문 파트너	<ul style="list-style-type: none"> • 메크로임팩트 02-3446-3508 	<ul style="list-style-type: none"> • (주)팩키시스템즈코리아 02-558-7170 	