

bintec X2250

Umfangreiche Routing-Funktionalitäten gepaart mit gesichertem kabellosen Netzzugang: der Wireless Router bintec X2250.

X2250

Mit dem Wireless Router bintec X2250 stellt Funkwerk Enterprise Communications erstmals ein Mitglied der bekannten bintec Routerfamilie mit einer Wireless Schnittstelle vor. Das Gerät verbindet die Leistungsmerkmale, wie sie schon aus den Produkten der X-Generation und VPN-Serie bekannt sind mit einer 802.11b/g WLAN Schnittstelle und ermöglicht somit auch einen kabellosen Zugang zum Netzwerk.



Kabelloser Netzzugang nach 802.11b/g

Der bintec X2250 arbeitet nach dem IEEE Standards 802.11g und überträgt die Daten mit 54 Mbit/s im 2,4 GHz Frequenzbereich. Aufgrund der Kompatibilität dieses Standards zur 11 Mbit/s Variante 802.11b ist es zudem möglich, den bintec X2250 auch in bereits existierenden 11 Mbit/s Umgebungen einzusetzen. In Verbindung mit den umfangreichen Leistungsmerkmalen ist es somit problemlos möglich, einen kabellosen und sicheren Zugriff auf Unternehmensressourcen oder einen mobilen Zugang zum Internet herzustellen.

Umfangreiche Sicherheitsmaßnahmen

Neben den umfangreichen mobilen Einsatzmöglichkeiten birgt die Datenübertragung über die Luftschnittstelle vor allem die Gefahren, die sich bei der Nutzung eines sog. shared medium ergeben. Da ein Zugang zu diesem Übertragungsmedium praktisch von jeder Stelle in der näheren Umgebung möglich ist, werden hier besonders hohe Anforderungen an die gesicherte Datenübertragung gestellt. Der IEEE Standard 802.11i, der speziell die Sicherheitsanforderungen im Bereich WLAN definiert, wird daher ebenfalls unterstützt. So bietet der bintec X2250 nicht nur eine Verschlüsselung nach WEP, sondern bietet zudem ein höheres Sicherheitsniveau durch die Unterstützung der 802.11i-konformen WPA Spezifikation. Zur weiteren Erhöhung der Sicherheit kann zudem durch Definition von MAC Filtern der Zugang zum WLAN bei Anmeldung eines Wireless Clients reglementiert werden.

Port-basierter LAN Zugang nach 802.1x

Viele Angriffe lassen sich bereits mit einfachen Mitteln realisieren, wenn ein Zugang zum lokalen Netz möglich ist. Wird diese Zugangsmöglichkeit bereits auf Port-Basis reglementiert – ganz gleich ob es sich hierbei um einen Ethernet oder Wireless Zugang handelt – so lässt sich hierdurch eine erhöhte Sicherheit für das lokale Netz erzielen. Der entsprechende Standard zur Port-basierten Authentifizierung wird als 802.1x bezeichnet und wird ebenfalls durch den bintec X2250 unterstützt. 802.1x verwendet EAP (Extensible Authentication Protocol) für die Übertragung von Authentifizierungsinformationen zwischen Access Point und einem Radius Server. Der bintec X2250 unterstützt eine Vielzahl von EAP Varianten und bietet daher größtmögliche Flexibilität für die Einbindung einer 802.1x-basierten Zugangskontrolle.

Starke Verschlüsselung durch WPA

Der erste Ansatz einer sicheren Datenübertragung für WLANs wurde durch das Protokoll WEP (Wired Equivalent Privacy) festgelegt. Es zeigte sich jedoch sehr bald, dass das hierbei eingesetzte Verschlüsselungsverfahren in Verbindung mit den Schlüssellängen einige Schwachstellen aufzuweisen hatte und bereits durch Einsatz herkömmlicher Softwaretools geknackt werden kann. Um diese Schwächen des WEP-Protokolls zu umgehen, wurde frühzeitig mit WPA (Wi-Fi Protected Access) eine sichere Verschlüsselungsmethode für WLANs definiert. Der bintec X2250 bietet nicht nur eine Abwärtskompatibilität zu bestehenden WEP-verschlüsselten WLANs, sondern unterstützt weiterhin die sichere WPA-Verschlüsselung. Neben dem Einsatz eines preshared keys unter Verwendung des TKIP-Protokoll (Temporal Key Integrity Protocol) bietet WPA zudem die Möglichkeit zur Benutzer

Authentisierung nach 802.1x. Für den Einsatz in Unternehmensnetzen mit eigenem Radius-Server oder in SOHO-Umgebungen ist der bintec X2250 gleichermaßen geeignet, da er sowohl den WPA-Enterprise-Modus als auch den WPA-PSK Modus unterstützt. Hierdurch bietet der bintec X2250 für Anwendungsszenarien jeglicher Größe einen optimalen gesicherten Zugang zum WLAN.

Definition unterschiedlicher Benutzergruppen

In der Vergangenheit war es bisher nur möglich, pro wireless Interface ein WLAN zu definieren, welches eindeutig durch die SSID (Service Set Identifier) klassifiziert wurde. Mit der Unterstützung des Multi-SSID Verfahrens bietet der bintec X2250 nun die Möglichkeit, mehrere WLANs pro Interface zu definieren und somit die verschiedenen Sicherheitsanforderungen auch für WLANs zu ermöglichen. Durch die Zuweisung zu einer eigenen SSID kann einer Benutzergruppe eine eigene Sicherheitsrichtlinie zugeordnet werden. Entsprechend den Anforderungen kann hierbei individuell die Form der Authentisierung oder Verschlüsselung festgelegt werden. So lässt sich z.B. ein interner Netzzugang über MAC Filter und WPA Radius Authentisierung parallel zu einem unverschlüsselten Internet Zugang über einen bintec X2250 realisieren.

Bestmöglicher Empfang

Zur Sicherstellung eines optimalen Kommunikationsverhaltens über die Luftschnittstelle ist der bintec X2250 mit einem Duo-Antennen ausgestattet. Beide Empfänger sind auf den gleichen Frequenzbereich ausgerichtet und ermöglichen über die Funktion Antenna Diversity eine optimierte Empfangsbereitschaft. Da bereits leichte Veränderungen in der direkten Umgebung oder kleinste Standortveränderungen eines Wireless Clients ein unterschiedliches Empfangsverhalten für den bintec X2250 bewirken können, sind die beiden Antennenempfänger derart aufeinander ausgerichtet, dass die Kommunikation über die Antenne mit den jeweils besten Empfangseigenschaften abgewickelt wird.

Aufbau kabelloser Infrastrukturen

Mit der Unterstützung des WDS Verfahrens (Wireless Distribution System) bietet der bintec X2250 die Option einer kabellosen Verbindung zwischen zwei WLAN Zugangspunkten. Auf diese Weise lässt sich eine kabelgebundene Infrastruktur an Punkten erweitern, in denen die Verlegung weiterer Trassen nicht kosteneffizient oder technisch nur schwer realisierbar erscheint. Die hierbei erzielbare Flexibilität durch den Einsatz der WDS-Funktionalität kann z.B. ausgenutzt werden, wenn Büroflächen zu verbinden sind, die durch einen öffentlichen Platz getrennt werden.

Gewohnter Leistungsumfang

Neben den neuen Wireless Funktionalitäten bietet der bintec X2250 als Wireless Router den gewohnten Leistungsumfang bisheriger bintec Router. So besitzt das Gerät neben zwei Fast Ethernet Schnittstellen einen ISDN Anschluss, der z.B. bei Ausfall der WAN Anbindung für ein ISDN-Backup verwendet werden kann. Die Sicherheit des lokalen Netzes wird durch die integrierte Firewall Funktion bereitgestellt. Für den Aufbau einer gesicherten VPN Verbindung verfügt der bintec X2250 bereits über 5 nutzbare IPSec Tunnel, weitere Tunnel können per Lizenz freigeschaltet werden. Die Konfiguration der Geräte erfolgt entweder über den HTTP Configuration Wizard (für ungeübte Anwender empfohlen) oder über eine HTML Oberfläche. Eine absolut sichere Konfiguration erlaubt die SSH verschlüsselte Kommunikation zum Gerät.

Wireless LAN

Merkmal	Bezeichnung
Standards	IEEE802.11b bzw. IEEE802.11g
Kanäle	13 Kanäle (Europa) bzw. 11 Kanäle (USA)
Sendeleistung	max. 100 mW (20 dBm) eirp.
WDS	verfügbar
WLAN	WEP64 (40 Bit Schlüssel), WEP128 (104 Bit Schlüssel), MAC Adress Filterung, Multi-SSID, WPA PSK (TKIP Encryption), WPA Radius
Authentication	802.11i (802.1x/EAP-MD5), 802.11i (802.1x/EAP-TLS), 802.11i (802.1x/EAP-TTLS), 802.11i (802.1x/EAP-PEAP), 802.11i (Key Management), 802.1x/EAP

ISDN-Schnittstelle

Merkmal	Bezeichnung
ISDN-Protokolle	Euro-ISDN und weitere nationale ISDN-Protokolle
Wähl- und Festverbindungen (S0)	Unterstützte Festverbindungen: D64S, D64S2, TS02, D64S2Y
B-Kanal-Protokolle	Hervorragende Interoperabilität mit anderen Herstellern (Raw-HDLC, CISCO-HDLC, X.75)
PPP, ML-PPP	(Siehe Software)
Multi-CAPI	Optional: CAPI 2.0 mit CAPI-User-Konzept (Passwort für CAPI-Nutzung) ermöglichen direkten Zugriff auf z.B. Fax- und E-Mail-Dienste
Bitraten-Adaption	V.110 (1.200 bis zu 38.400 Bit/s), V.120 bis 57.600 kBit/s (HSCSD) zur Verbindung mit GSM-Teilnehmern

Sicherheit

Merkmal	Bezeichnung
NAT/PAT	Network & Port Address Translation / Stateful Packet Inspection: Abschottung des gesamten Netzes vom öffentlichen Zugang
CLID und Callback	Identifizierung des Anrufers (CLID), Rückruf (Callback)
Access-Listen	Filtern von IP-Paketen nach unterschiedlichen Kriterien (Source, Destination, Port und Interface)
Stateful Inspection Firewall	Filterung mit Überwachung und Interpretation des jeweiligen Status der einzelnen Verbindungen
RADIUS	Zentrale Überprüfung der Zugangsberechtigung auf einem RADIUS-Server (PPP und Login Authentifizierung)
TACACS+	Unterstützung von TACACS-Servern zur Authentifizierung, Autorisierung und Abrechnung (AAA) von Benutzern
Authentisierung	PPP-Mechanismen (siehe Software)
H.323-Proxy	Schutz des Intranets (z.B. durch NAT)
VLAN	Netzwerkknoten lassen sich aus verschiedenen Netzwerksegmenten zu Arbeitsgruppen zusammenfassen
Verschlüsselung für PPP	MPPE bis zu 128 bit, andere bis zu 168 bit
VPN - IPsec	Bis zu 5 Tunnel inklusive, weitere Tunnel über optionale Lizenz
VPN - IPsec	Starke Verschlüsselung bis 256 Bit (AES, 3DES, DES, CAST, Blowfish, Twofish)
VPN - PPTP	Optional
VPN - PPTP	Starke Verschlüsselung bis 128 Bit (MPPE), bis zu 168 Bit (DES/3DES, Blowfish)
DynDNS / DynVPN	Router ist trotz dyn. IP-Adresse über das Internet erreichbar
IKE für IPsec	Pre-Shared Keys und Support von X.509-Zertifikaten
X.509	X.509 v1/v3 Zertifikate (PKCS#7/8/10, 12, CLRs, SCEP)
QoS für IPsec	Verfügbar
PKI Support für IPsec	Verfügbar
NAT Traversal für IPsec	Verfügbar
Dynamisches IPsec im B- und	Verfügbar, kostenlose Lizenz erforderlich
IPCOMP	IP Kompression
IPsec / RADIUS	Verfügbar
IPsec Redesign	Policy Manager und Interface-Konzept
L2TP	Layer-2 Tunneling Protokoll für ATM, Ethernet, PPP; Benutzer-Authentifikation

Wartung und Service

Merkmal	Bezeichnung
ISDN-Logging	ISDN Event & System Logging: Aufzeichnung von Systemmeldungen und Ereignissen, z.B. Einbruchsversuchen
SNMP	Komplettes Management mit MIB-II, Enterprise-MIB, inklusive SNMP-Management-Software für Windows (DIME-Tools und -Browser)
SSH Login	Für sichere Verbindungen von Terminal Anwendungen
Lokale / remote Wartung	Komplette Konfiguration und Wartung, lokal und aus der Ferne, über Ethernet, ISDN-login oder serieller Schnittstelle
Trace / Debugging / Monitoring	Traces für ISDN B-/D-Kanal, R-CAPI-Traces, Ethernet-Traces, Grund für Verbindungsabbruch, ISDN-Signalisierungsinformation
Email Alert	Vorhanden
DHCP	Server und Client zur vereinfachten Konfiguration für TCP/IP
Setup-Tool	Integriertes, menü-basierendes, intuitiv zu bedienendes Setup-Programm, einheitlich für das gesamte Bintec Produkt-Portfolio
HTML-Setup-Tool	Grafische Benutzeroberfläche für Browser mit Java Script
HTML Wizard	Browser-basierter Konfigurations-Assistent
H.323-Gatekeeper	Kommunikationskontrolle zwischen Gateway und H.323-Endgeräten
XADMIN	Roll out tool für größere Router-Installationen (IP+ISDN)
Activity Monitor	Kontrolle der Router-Aktivitäten von jedem LAN-PC aus
Dokumentation	Deutschsprachige Dokumentation auf CD
Gewährleistung	2 Jahre Hersteller-Gewährleistung

Software-Ausstattung

Merkmal	Bezeichnung
TCP/IP-Routing	Routing-Information-Update und -Verteilung statisch oder dynamisch (RIP v1/v2/triggered, RFC 2091), selektierbar für jedes Interface, ProxyARP, BOOTP/DHCP- Forwarding
Erweitertes IP-Routing	Abhängig von Quell-/Zielpport, Source-IP-Address, TOS ..., d.h. Policy Based Routing
OSPF	Statische/dynamische Aktualisierung und Verteilung von Routing-Informationen
Bridging	Spanning Tree & Transparent Mode
QoS	Quality of Service mit DiffServ und Shaping: Trennung des IP-Datenverkehrs in Klassen mit verschiedenen Prioritäten, optimiertes Queue-Handling und Shaping gemäß diesen Prioritäten
TCP Download Rate Control	Optimieren des Download Verhaltens für VoIP
BRRP	Bintec Router Redundancy Protocol, Backup eines Router-Services durch einen anderen Router im LAN (Virtual Router)
IP Load Balancing	Bandwidth Management
BoD	Bandwidth on Demand: skalierbare Bandbreite, dynamische Bandbreitenzuschaltung in Abhängigkeit vom Datenaufkommen
AUX Backup	Backup-Möglichkeiten über GSM, GPRS oder Analog-Modem
PPP	Authentisierungsmechanismen (PAP, CHAP, MS-CHAP, MS-CHAP v2), Standard PPP, Kanalbündelung über Multilink-PPP (ML-PPP), transparent Mode, dynamische IP-Adressvergabe (Server- und Client-Modus)
PPPoE	Point to Point Protocol over Ethernet (Client und Server) für High-speed Internet-Zugang über xDSL (RFC 2516)
Dyn. IP-Adressen	Einfacher Internet-Zugang ohne feste IP-Adressen
Artem Access Point Discovery	Auffinden von konfigurierten und unkonfigurierten Artem Access Points im LAN
ISDN-Accounting	Detaillierte laufende Aufzeichnung (Call Detail Recording), Rufnummer, Gebühreninformation, ...
IP-Accounting	Source, Destination, Port, Interface, Pakete/Bytes-Zähler
Event Scheduler	volumenabhängige oder zeitbasierte Budgets möglich
Shorthold	Statischer und dynamischer Shorthold spart Verbindungskosten durch automatischen Verbindungsabbau
Keep Alive Monitoring	spart Kosten, indem ein Verbindungsaufbau nur zugelassen wird, wenn konfigurierbare IP-Adressen erreichbar sind
MPPC	Software-Datenkompression auch in Verbindung mit MPPE (Microsoft Point to Point Encryption), kostenlose Lizenz erforderlich
STAC	Kompression für PPP-Verbindungen, kostenlose Lizenz erforderlich
Cost-of-Ownership	Minimal durch z.B. kostenlose Software-Updates, komplette Fernwartbarkeit

Hardware-Ausstattung

Merkmal	Bezeichnung
RISC Architektur	Motorola 8241 RISC Prozessor mit 32 MB RAM
Flash-ROM	8 MB on board
LAN / WAN	2 x 10/100 MBit/s Ethernet Twisted Pair, autosensing
WLAN	Internes Radiomodul, 2,4 GHz Band, 2 externe Antennen (Antenna Diversity)
ISDN	1 x S0, 2 B-Kanäle
Konsole	Serieller Konsole-Port: RS 232 C, 8pol. Mini-DIN, 1.200 Bit/s - 115 kBit/s
Netzteil	Externes Trafo-Netzteil 12 V DC, 1 A
Ein/Aus-Schalter	Vorhanden
Status-LEDs	Power, Status, Ethernet 1, Ethernet 2, ISDN-D, ISDN-B, WLAN
Wandhalterung	Optional montierbar
Metall-Gehäuse	Vorhanden
Abmessungen	Ca. 200 x 30 x 150 mm (B x H x T)
Gewicht	Ca. 900 g