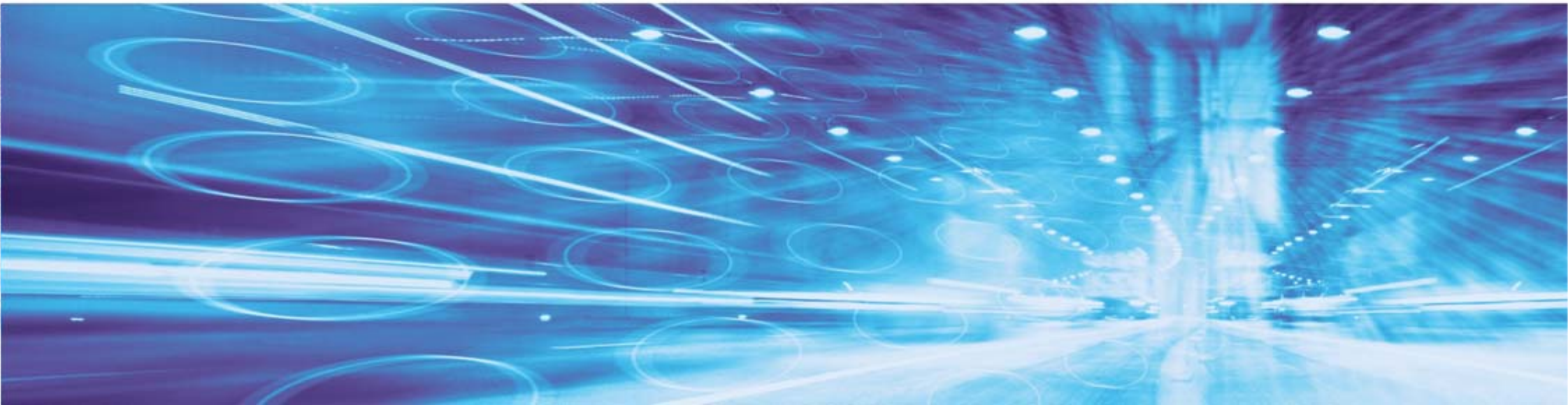




SICHERE UND STABILE WIRELESS-LAN INFRASTRUKTUREN



DDS NETCOM





SICHERE WIRELESS LAN INFRASTRUKTUR ALLGEMEINES

Wireless-LAN bedeutet einen kaum zu überbietenden Komfort.

Jeder Notebook, Laptop oder PDA hat heute eine Wireless-LAN Schnittstelle.

70% der privaten WLAN- Funknetze sind ungesichert!

Gefahren: Ungenügend geschützt übertragene Daten können mitgelesen und/oder manipuliert werden - ungenügend geschützte WLAN-Zugänge können missbraucht werden!



SICHERE WIRELESS LAN INFRASTRUKTUR ACCESSPOINT SICHER VERWALTEN

Kabelverbindung oder zumindest verschlüsselte Funkverbindung zum Verwaltungs- Tool (z.B. Webseite) des AccessPoints verwenden.

Standard-Passwort ändern, sicheres, eigenes Passwort verwenden.

Remote-Administration ausschalten.

Cisco Aironet 1130AG Series Access Point

Hostname: WVO-IP-5D4FC3 16:52:43 Wed Jun 2 2010

Home: Summary Status

Association	
Clients_1	Roamstata_2

Network Identity	
IP Address	192.168.1.220
MAC Address	0014.0000.5000

Network Interfaces		
Interface	MAC Address	Transmission Rate
Event Log		
Time	Severity	Description
Jun 2 14:11:23.000	Information	Interface Port 18/40/03: Reauthentication Station



SICHERE WIRELESS LAN INFRASTRUKTUR FIRMWARE UND SOFTWARE AKTUALISIEREN

Es gibt praktisch keine fehlerfreie Software, daher lohnt es sich, die aktuellen Firmware-Sicherheitsupdates einzuspielen.

Auch Hardware-Treiber und proprietäre WLAN-Software aktualisieren.





SICHERE WIRELESS LAN INFRASTRUKTUR BESTMÖGLICHE VERSCHLÜSSELUNG EINSETZEN

Der Datenverkehr muss vor unbefugtem Zugriff geschützt werden, daher ist die Verschlüsselung der übertragenen Daten und die Authentifizierung der Benutzer unabdingbar.

WEP: Besser als gar nichts.... legt potentiellen Einbrechern wenigstens einen Stolperstein in den Weg.

WPA: Ergänzt WEP um dynamische Schlüssel, daher ist das Dechiffrieren des Datenverkehrs erheblich erschwert. Schutzgrad hängt von der Komplexität der Passphrase ab; Je länger das Passwort, umso besser.

WPA2: Weiterentwicklung von WPA, derzeit der beste Schutz. Verwendet AES als Verschlüsselungsalgorithmus.



SICHERE WIRELESS LAN INFRASTRUKTUR SSID ÄNDERN UND BROADCAST UNTERBINDEN

Standard-SSID ändern, keine SSID konfigurieren, die auf den WLAN- Betreiber Rückschlüsse erlaubt.

SSID-Broadcast- Option wenn möglich deaktivieren um zu verhindern, dass der Name des WLAN-Netzes andauernd in den Äther gesendet wird.

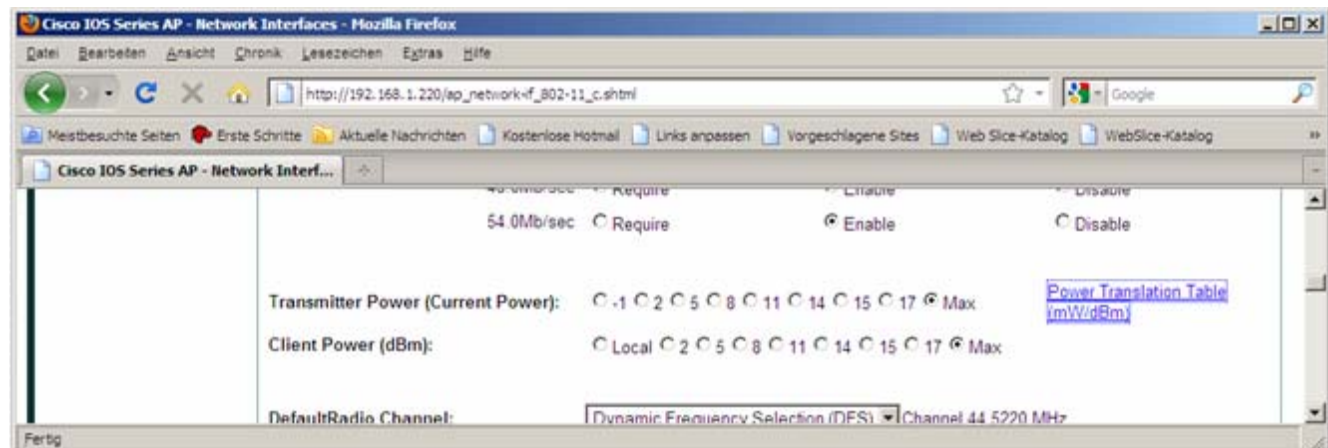
SSID mit <\> am Anfang verwenden.



SICHERE WIRELESS LAN INFRASTRUKTUR REICHWEITE DES WLAN- FUNKSIGNALS BESCHRÄNKEN

Eine Sendeleistung, die eine Kommunikation über die räumlichen Grenzen des geplanten Nutzungsbereichs hinaus ermöglicht, ist nicht sinnvoll.

Allenfalls mit Richtfunk-Antennen den Sendebereich einschränken.





SICHERE WIRELESS LAN INFRASTRUKTUR AUTHENTIFIZIERUNG

DHCP auf dem AccessPoint deaktivieren und MAC- Filter einsetzen, um einen unerlaubten Zugriff zu erschweren

Wenn möglich und sinnvoll, IEEE 802.1x- Authentifizierung und/oder OneTime-Passwort Token verwenden.





SICHERE WIRELESS LAN INFRASTRUKTUR FIREWALL UND LOGBUCH AKTIVIEREN

On-Board Firewalls und/oder Paketfilter unbedingt aktivieren, dies hebt das Schutzniveau des Netzwerk erheblich.

Logbuch ab und zu anschauen, bei erfolgreichen Netzwerkanmeldungen von unbefugten Nutzern ist es an der Zeit, strengere Sicherheitsvorkehrungen zu treffen!

Time	Severity	Description
Jun 2 14:12:18.675	Information	Interface Dst-Wlan0: Deauthenticating Station 0125:8361:8956 Reason: Standing station has left the BSS
Jun 2 14:00:48.852	Information	Interface Dst-Wlan0: Station 0121:8361:8956 associated KEY: 8021F9A34E
Jun 2 14:08:12.235	Warning	Packet to card 01% 7734:012F reached max retries, removing the client
Jun 2 14:08:12.229	Information	Interface Dst-Wlan0: Deauthenticating Station 0116:7734:012F Reason: Previous authentication no longer valid
Jun 2 14:08:12.228	Warning	Packet to card 01% 7734:012F reached max retries, removing the client
Jun 2 14:07:00.162	Information	Interface Dst-Wlan0: Station 1010:012F:012F associated KEY: 8021F9A34E
Jun 2 14:00:18.208	Information	Interface Dst-Wlan0: Deauthenticating Station 0125:8361:8956 Reason: Standing station has left the BSS
Jun 2 14:00:08.232	Information	Interface Dst-Wlan0: Station 0121:8361:8956 associated KEY: 8021F9A34E
Jun 2 14:11:23.098	Information	Interface Dst-Wlan0: Deauthenticating Station 0125:8361:8956 Reason: Standing station has left the BSS
Jun 2 14:10:08.438	Information	Interface Dst-Wlan0: Station 0125:8361:8956 associated KEY: 8021F9A34E



SICHERE WIRELESS LAN INFRASTRUKTUR FAZIT

Alle genannten Massnahmen garantieren noch kein absolut sicheres WLAN, sie erschweren einen Missbrauch jedoch in einem Umfang, so dass nur mit sehr grossem technischem Aufwand und erheblicher krimineller Energie in ein WLAN eingebrochen werden kann.

Kabelgebundene Datenübertragung kann auch abgehört und/oder manipuliert werden, meistens werden solche Daten unverschlüsselt übertragen!

Die allgemeine Verfügbarkeit von kabelgebundener Kommunikation ist höher (das Übertragungsmedium ist gegen äussere Einflüsse weitgehend unempfindlich), „sicherer“ als die Übertragung über WLAN ist es aber sicher nicht.



SICHERE WIRELESS LAN INFRASTRUKTUR FAZIT

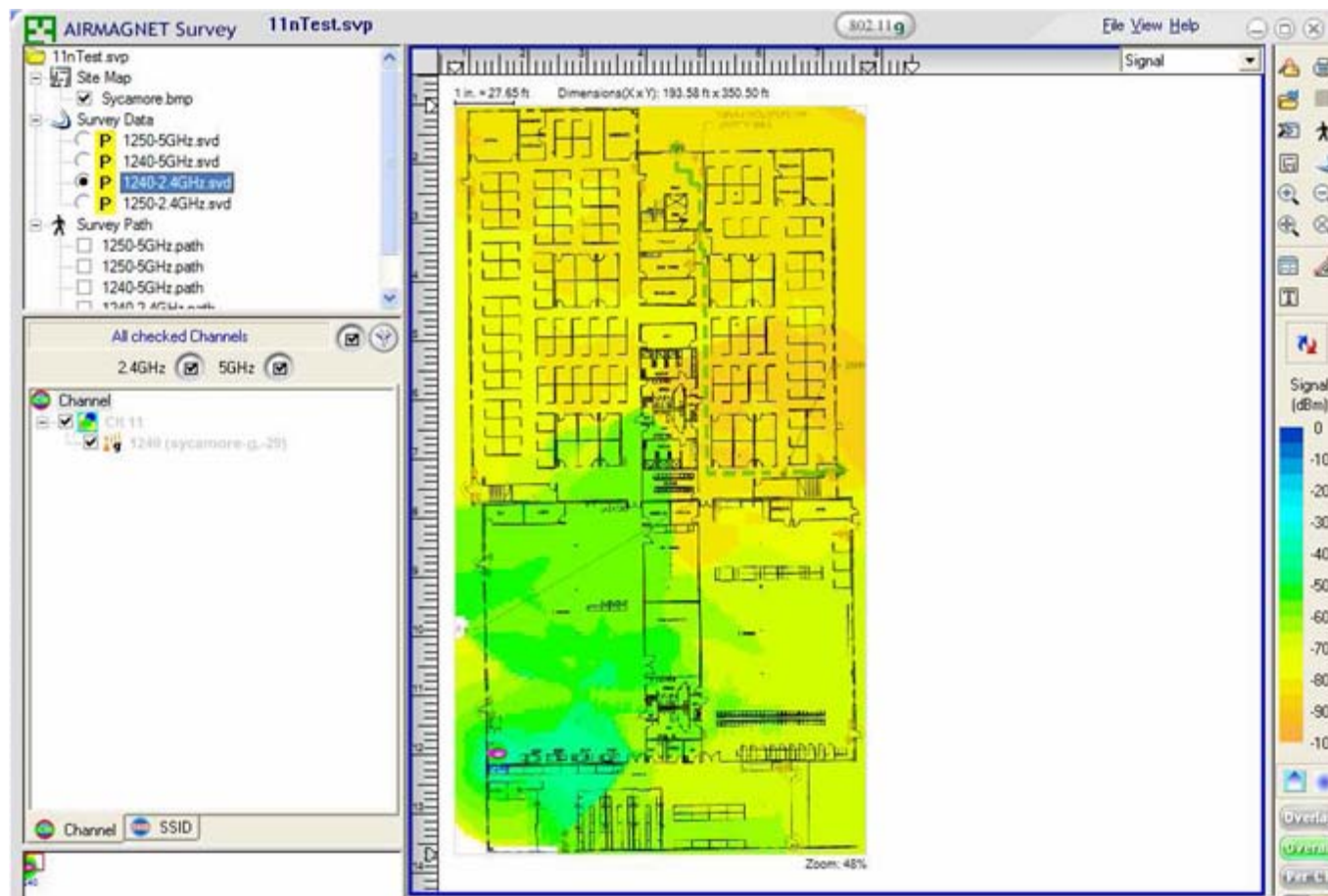
Wenn technisch möglich und sinnvoll: Verkabeln !

Ansonsten: Möglichkeiten von WLAN erkennen und Mehrwert nutzen !





WIRELESS LAN GRUNDLAGE: SITE SURVEY DURCHFÜHREN





DDS NETCOM

WIRELESS LAN STAND-ALONE ACCESSPOINT

Kleine Netzwerke, bis max. 3 AccessPoints (z.B. HomeOffice).
Jeder einzelne AccessPoint wird individuell konfiguriert

802.1x authentication, internal RADIUS server

WPA/WPA2 support

MAC Filter

Hide Name (SSID)

Dynamic channel selection

usw.





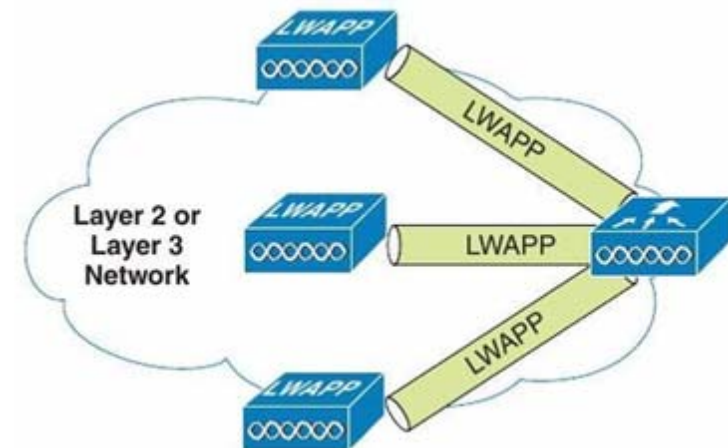
WIRELESS LAN

WIRELESS LAN MIT WLAN-CONTROLLER

Grössere Netzwerke, ab 3 bis 5 AccessPoints

WirelessLAN-Controller ist der zentrale „WLAN-Experte“ im Netzwerk, alle AccessPoints werden zentral gesteuert und verwaltet.

Alle vorher genannten Sicherheitsaspekte können zentral konfiguriert und verwaltet werden.

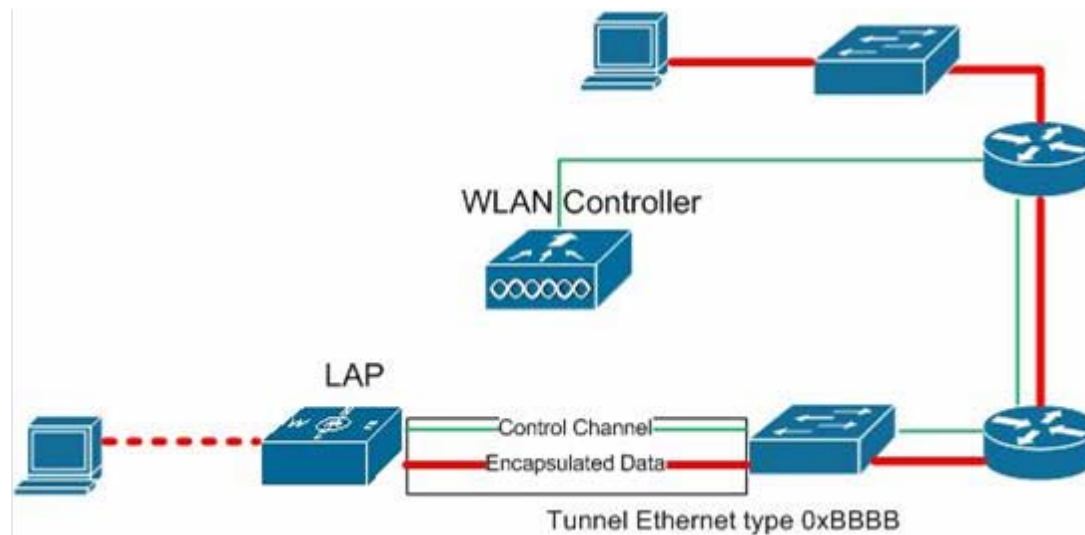




WIRELESS LAN

WIRELESS LAN MIT WLAN-CONTROLLER

LWAPP: Lightweight Access Point Protocol von Cisco Systems Inc.
Standard: IETF approved it in RFC 5412





WIRELESS LAN

WIRELESS LAN MIT WLAN-CONTROLLER

Wireless LAN Controller vereinfachen die Bereitstellung und den Betrieb von grösseren drahtlosen Netzwerken erheblich.

Wireless LAN Controller ermöglichen eine optimale Performance, mehr Sicherheit und eine höhere Verfügbarkeit des Netzwerks.

Wireless LAN Controller sind als Stand-Alone Geräte oder integriert in Router oder Switches verfügbar.





DDS NETCOM

MEHRWERT WIRELESS LAN NETZWERK- ZUGANG FÜR GÄSTE

Sicherer Internet- Zugang für Gäste bereitstellen.

Zur Verfügung stehende Bandbreite für Gäste beschränken.

Hot-Spot- Funktionalität bereitstellen.





DDS NETCOM

MEHRWERT WIRELESS LAN DATENERFASSUNG ÜBER WIRELESS LAN

Mobile Datenerfassung mit Barcodeleser für die Lagerbewirtschaftung

Aufnahme von Bestellungen im Restaurant

Datenübergabe von und an mobile Einrichtungen,
z.B. Automobilindustrie: Dokumentation der Testergebnisse
während der Fertigung und Prüfung.





DDS NETCOM

MEHRWERT WIRELESS LAN TELEFONIEREN ÜBER WIRELESS LAN

VoIP über WLAN funktioniert einwandfrei, es ist keine separate DECT-Infrastruktur notwendig !

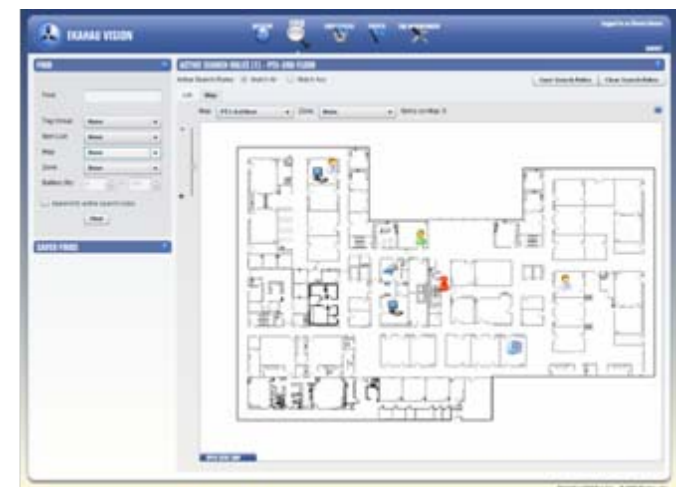




MEHRWERT WIRELESS LAN LOKALISIERUNG ÜBER WIRELESS LAN

Automatisches Auffinden von Personen und Gütern im gesamten Unternehmen
(z.B. im Spital, im Schulhaus usw.)

Benachrichtigung oder Alarmierung von Personen anhand definierter
Eventkriterien (Betreten und/oder Verlassen von Zonen, Batterieladestatus usw.)





DDS NETCOM

MEHRWERT WIRELESS LAN NETZWERKZUGANG FÜR MASCHINEN- UND GEBÄUDEWARTUNG

Effiziente Wartungsarbeiten direkt an der Maschine oder an der Steuerung.

Sichere Authentifizierung, Authorisierung und Reporting des Netzwerkzugriffs





DDS NETCOM

MEHRWERT WIRELESS LAN VIDEOÜBERWACHUNG

Einfache Überwachung und/oder Alarmierung.

Die Verbindung zur Kamera kann über einen Webbrowser oder über ein Video-Streaming erfolgen.





DDS NETCOM

MEHRWERT WIRELESS LAN VORTEILE

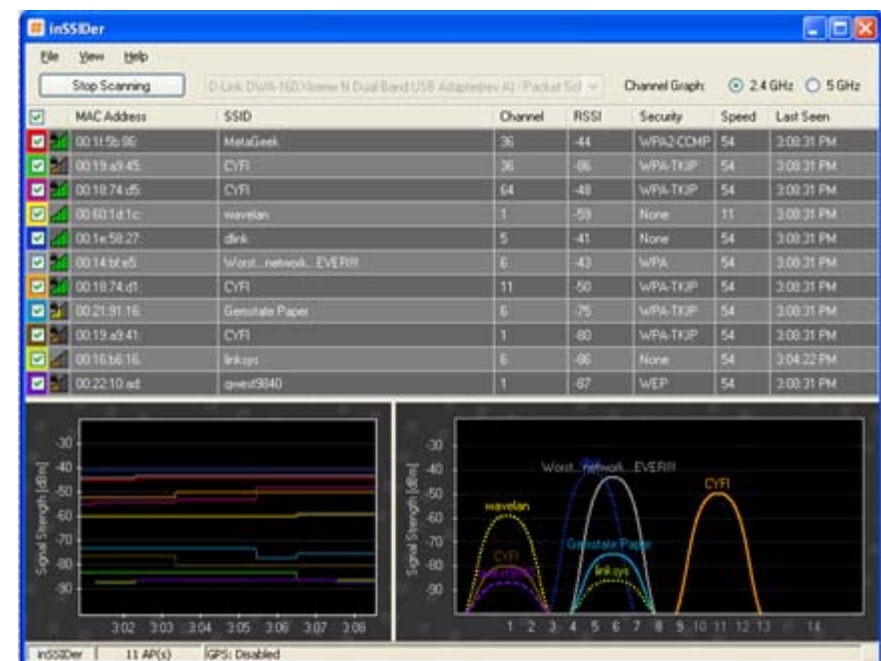
Erhöhung der Flexibilität

Einfache Erweiterbarkeit

Reduzierung von Installationskosten

Effizienzsteigerung im laufenden Betrieb

Reduzierung von Wartungskosten





DDS NETCOM

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT.

DDS NetCom AG
Hanspeter Weingartner, Projektleiter
Allmendstrasse 6
CH-8320 Fehraltorf

hanspeter.weingartner@dds.ch