

Feature Notes

LCOS 9.20 RC1



LCOS 9.20

Best Wi-Fi & maximum security for your network!

The new LCOS version 9.20 is a **massive package** that offers secure networking and top-quality Wi-Fi. Benefit from noticeable improvements in the performance and reliability of your access points and WLAN routers. Major new features also include **SNMPv3, IKEv2, and BGP** to take security in the areas of monitoring, site connectivity, and routing to an entirely new level.

LCOS 9.20
[LANCOM OPERATING SYSTEM]

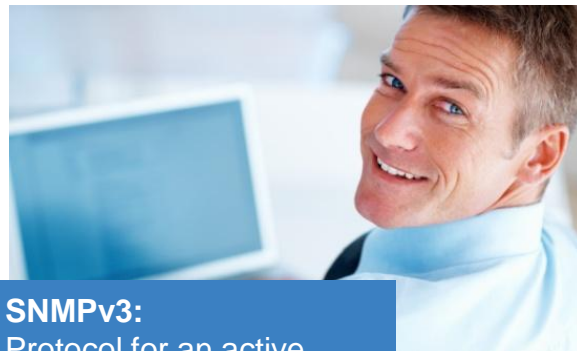


HIGHLIGHT

Support of SNMPv3 (Simple Network Management Protocol)

Improved security in network monitoring

- Encrypted monitoring and configuration via LCMS and LSM
- Comfortable and high-security device monitoring thanks to encrypted data communication
- Detection of interferences in the network and support for their elimination
- No configuration changes needed due to automatic activation

**SNMPv3:**

Protocol for an active support for the administrator in network management

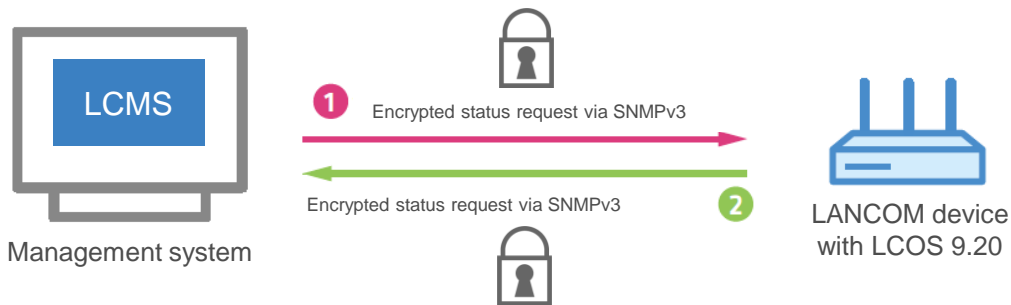
HIGHLIGHT

Support of SNMPv3

Differences to the previous versions SNMPv1 and SNMPv2

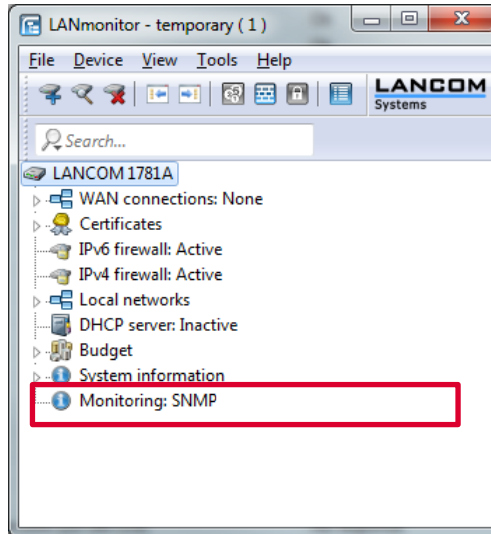
A decisive safety advantage due to:

- Encrypted data communication between network and management system
- Integrated user management with different user accounts for an optimal access control for configurations
- Precise control of administrator rights across different access levels

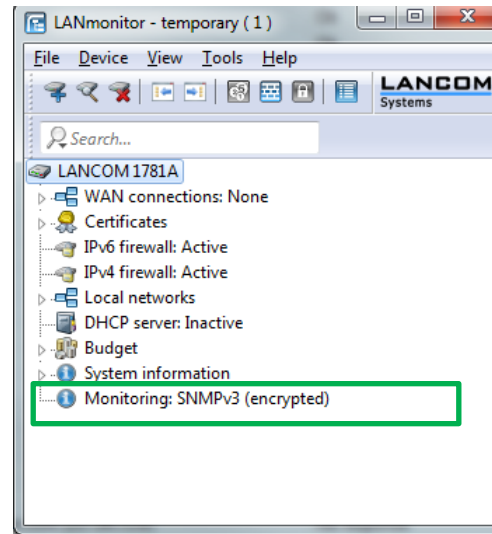


Support of SNMPv3 in LANmonitor

Before (without SNMPv3)
unencrypted



After (with SNMPv3)
encrypted



HIGHLIGHT

Maximum Wi-Fi Quality:

Best Wi-Fi for all access points, wireless routers, and WLAN controllers

Adaptive RF Optimization

Dynamic selection of the qualitatively best Wi-Fi channel in case of channel disturbances

Airtime Fairness

Improved utilization of the Wi-Fi bandwidth

Comprehensive quality improvements

The best Wi-Fi experience ever, thanks to noticeably more performance, robustness, and coverage



The next step of LANCOM Active Radio Control



Now available for all LANCOM WLAN controllers and wireless routers!



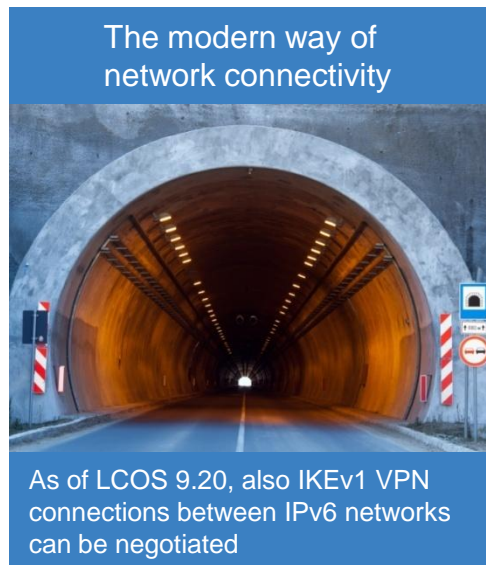
Activate the full potential of your wireless LAN!

Thanks to the intelligent combination of innovative features, included in our operating system LCOS, such as Band Steering, Adaptive Noise Immunity, Adaptive RF Optimization, Airtime Fairness, and Client Steering, the Wi-Fi performance is sustainably increased – and the administrator is supported with professional WLAN management.

IKEv2

Faster and more secure establishment of VPN tunnels

- Version 2 of the Internet Key Exchange Protocol (IKEv2)
- Flexible, encrypted networking of IPv4- or IPv6-based locations – even in mixed operation
- Faster thanks to more efficient protocol negotiation
- IKEv2 is already supported by many devices



IKEv2

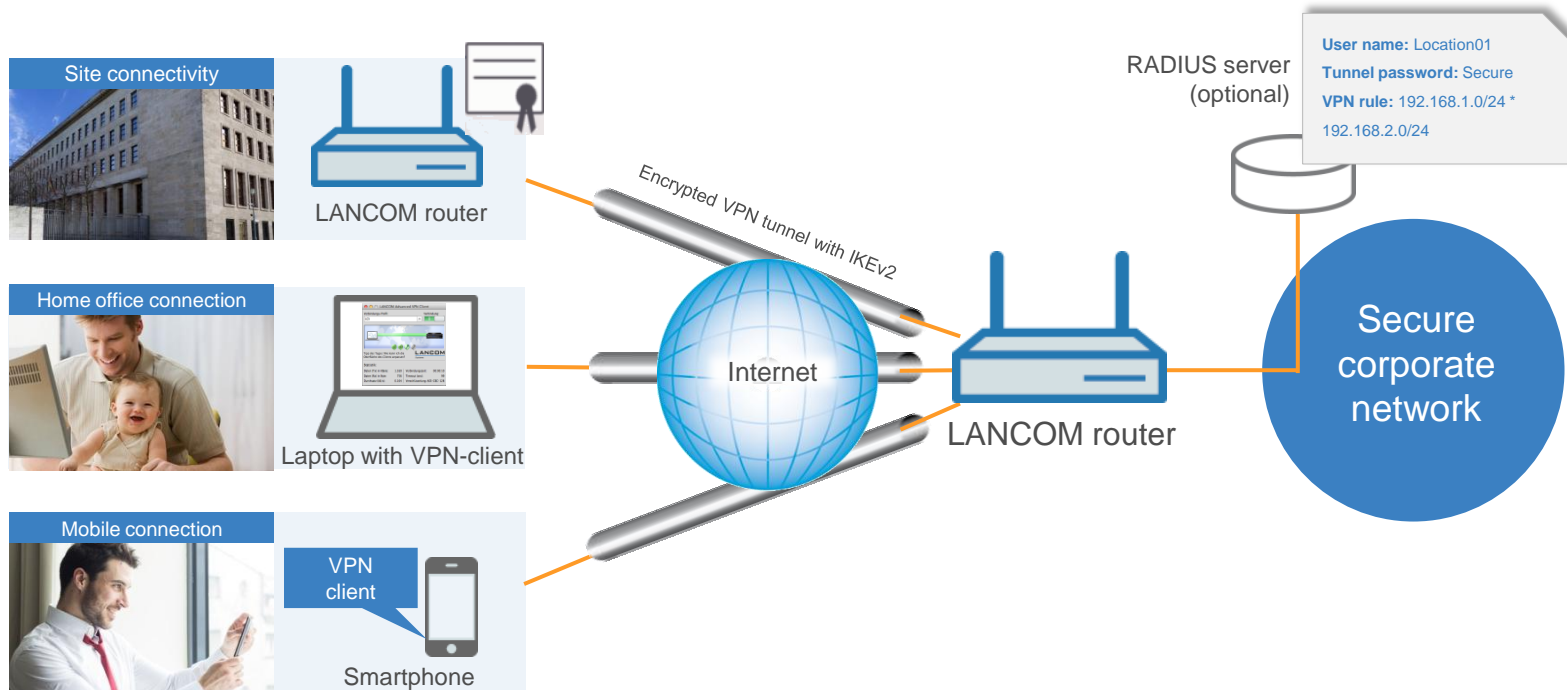


Note: IKEv1 and IKEv2 provide the same security when creating VPN connections!

Differences between IKEv1 and IKEv2

	IKEv1	IKEv2
Process	Main Mode Aggressive Mode	Only one defined process
Numbers of packet exchange	Main Mode → 9 Aggressive Mode → 6	only 4
Authentication process	same authentication on both sides	each remote site can use various authentication methods (for example: pre-shared key, Responder RSA Sig)
Security Association lifetimes	agreement of both sides required	not set, anyone can remove SA anytime

IKEv2 – Scenario



IKEv2 – supported features

> Operating modes

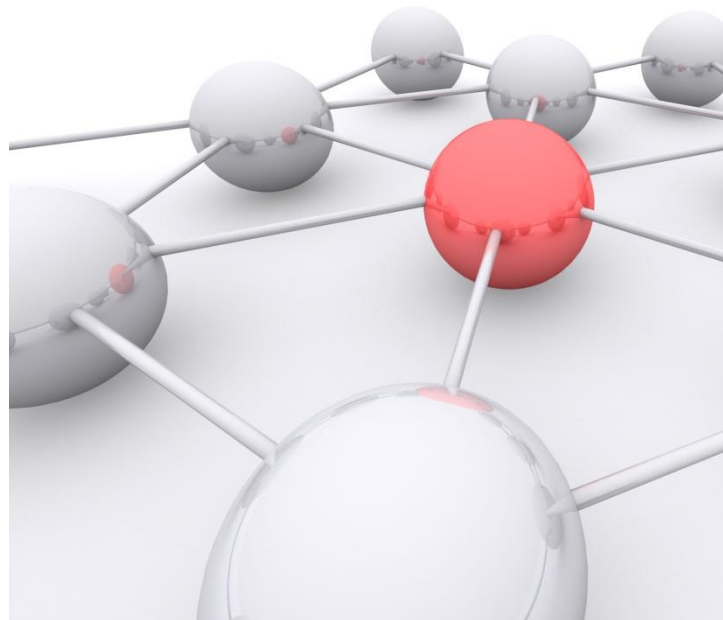
- › Site-to-site: connection between two routers
- › CFG-mode server: Dial-in from mobile clients with address assignment by the router
- › CFG-mode client: Dial-in as a client with the address reference from another router

> Authentication methods:

- › Digital certificates (RSA Signature)
- Pre-shared keys (passwords)

> Storage location of VPN configurations:

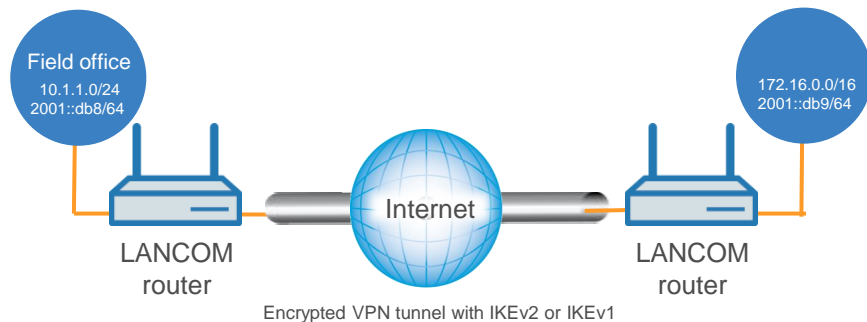
- › Within router
- › In the external RADIUS server (support of authorization and accounting)



IKEv2 with IPv6 support

New: VPN networking of IPv6 networks

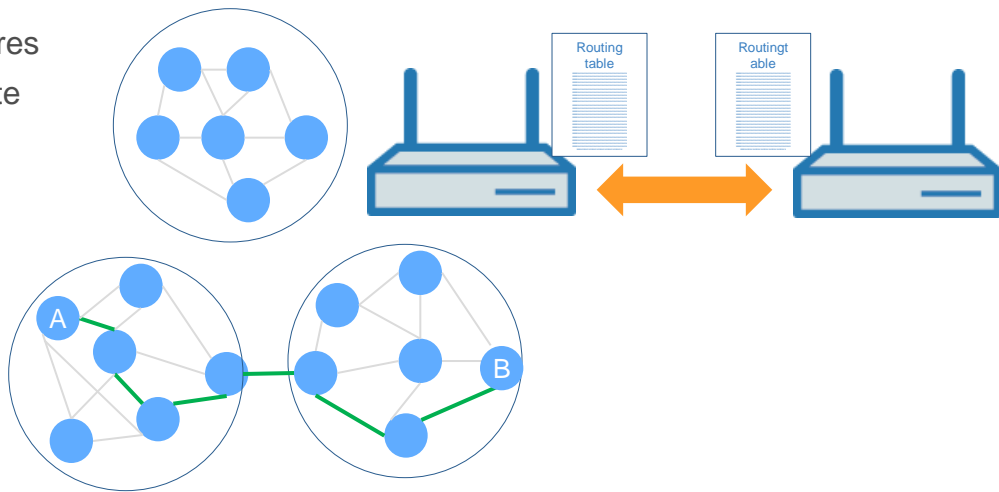
- Possible either via IKEv1 or IKEv2
- Network relations (IPv4 and IPv6) can be comfortably configured via a new network rule table
- Dial-in clients are also supported
- Parallel operation of IPv4 and IPv6 networks



BGP (Border Gateway Protocol)

Efficient VPN connectivity due to dynamic routing

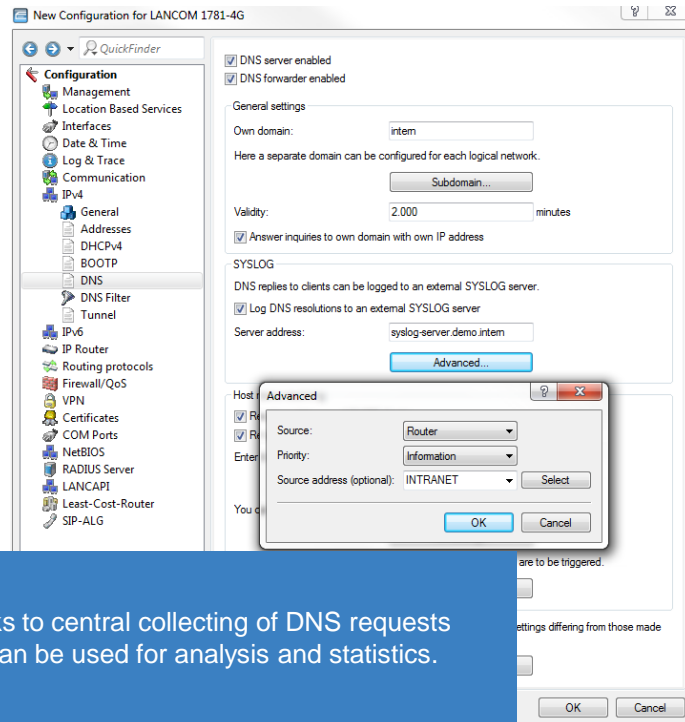
- BGP (Border Gateway Protocol) ensures that all networked routers communicate effectively by sharing the best paths from their routing tables



Logging of DNS requests

Analysis of online activities

- DNS requests from clients can be sent to an external SYSLOG server for logging and evaluation purposes



Thanks to central collecting of DNS requests they can be used for analysis and statistics.

Professional network analysis with iPerf

Performance measurement with iPerf

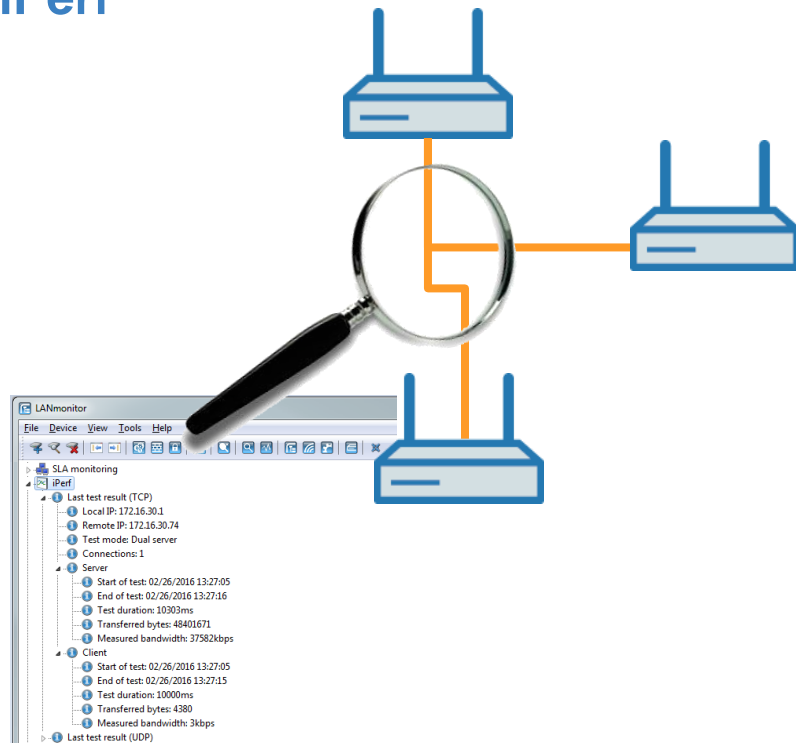
- Measurement of the maximum TCP and UDP throughput between two devices on the network
 - Maximum performance of a connection
 - Detection and amendment of bottlenecks in the network



Measurement of the throughput
Measuring the current throughput between 2 devices.



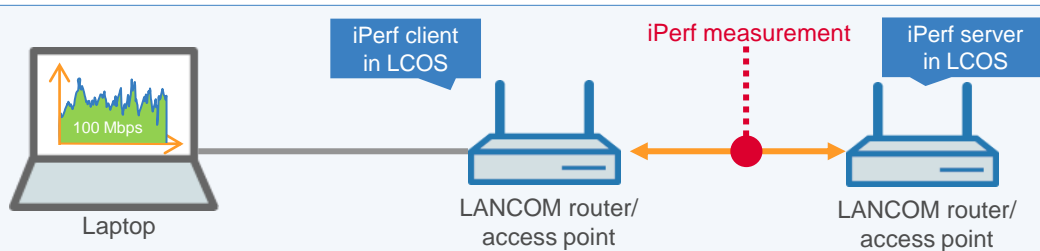
Detection and amendment of bottlenecks
Discrepancies can be revealed as a network bottleneck and be fixed as a result.



iPerf scenarios

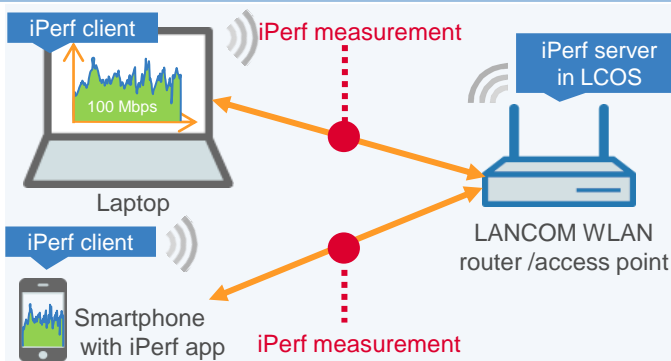
Scenario 1

Measurement between two LANCOM devices



Scenario 2

Measurement between end device and LANCOM device



Higher complexity for device passwords

New password policies

- › Increased safety in the use of passwords by activation of the new password policies
 - › Minimum eight characters
 - › Use of letters, numbers, and special characters

Example: H8X%tj7)



ICMP SLA-Monitor

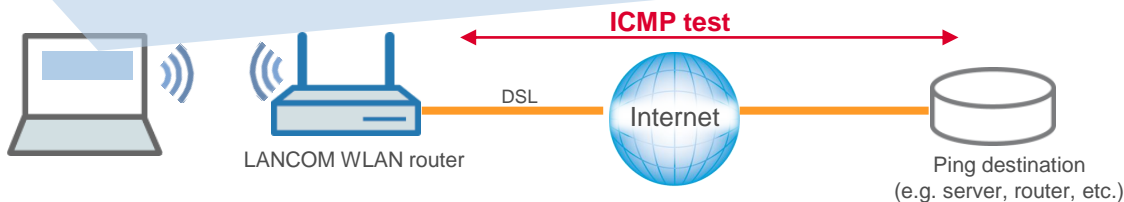
Performance measurement of connections



SLA = Service Level Agreement

SLA monitoring testresults of Aussenstelle

Index	Timestamp	Name	Destination	Packetloss	Minimal round trip time	Maximum round trip time	Average round trip time	Warning due to ...	Critical due to ...
653	02/25/2016 11:57:08	LCS	172.16.20.1	0	64.224000	112.063000	86.772000	Maximum round trip time,...	
654	02/25/2016 11:57:38	LCS	172.16.20.1	0	119.784000	313.041000	214.234000	Maximum round trip time,...	Maximum round trip time, ...
655	02/25/2016 11:58:07	LCS	172.16.20.1	0	36.602000	64.678000	42.733000		
656	02/25/2016 11:58:37	LCS	172.16.20.1	0	36.557000	46.497000	38.701000		



- Regular ping tests of network destinations
- Documentation of the results: packet round time, packet loss
- Warning when exceeding the results via SYSLOG or LANmonitor

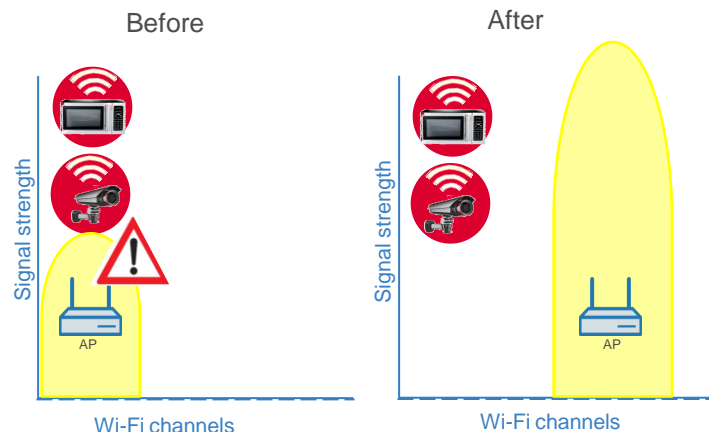


WLAN improvements

Adaptive RF Optimization

Dynamic selection of the optimal Wi-Fi channel

- Access point continuously scans the channel for sources of interference
- If serious sources of interference are recognized in the radio field which no longer enable normal operation, the access point dynamically switches to a better channel
- The channel change takes place during operation without the intervention of the administrator



Operational mode channel Configuration	When will channel changes take place?		
Static	---		
Automatic	When the access point starts up	✓	recommended
Dynamic	After the identification of serious interferences in the current channel	✓	recommended

Airtime Fairness

Example:

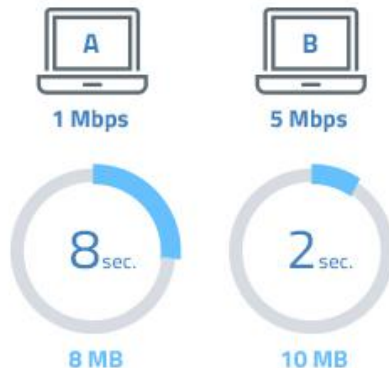
> Without Airtime Fairness:

Active clients are granted transmission times one after another – without a targeted partitioning of transmission times

> With Airtime Fairness:

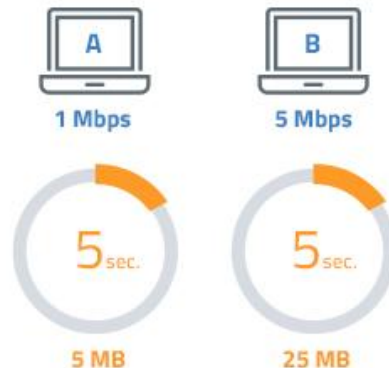
The available bandwidth is effectively utilized among active clients due to a fair sharing of Wi-Fi transmission times

Without Airtime Fairness



WLAN PERFORMANCE
18 MB data transmission
in 10 seconds

With Airtime Fairness



WLAN PERFORMANCE
30 MB data transmission
in 10 seconds

Airtime Fairness

Configuration options at a glance

› Equal Airtime (Default)

- › Equal distribution of Wi-Fi transmission times among active clients
- › Fast clients can transmit more data at the same time

› Equal Volume

- › All clients achieve the same data throughput
- › Slow clients get more time than fast clients

› Prefer 11n Airtime

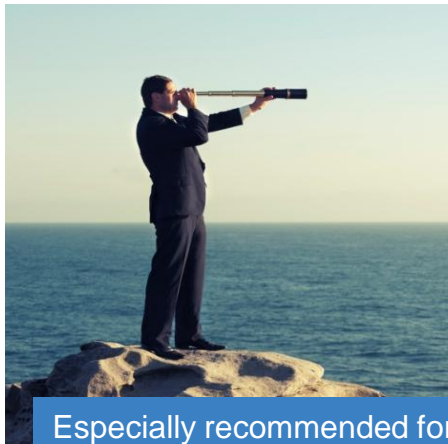
- › Fast clients can be prioritized over slow clients, so finishing their data transmission more quickly



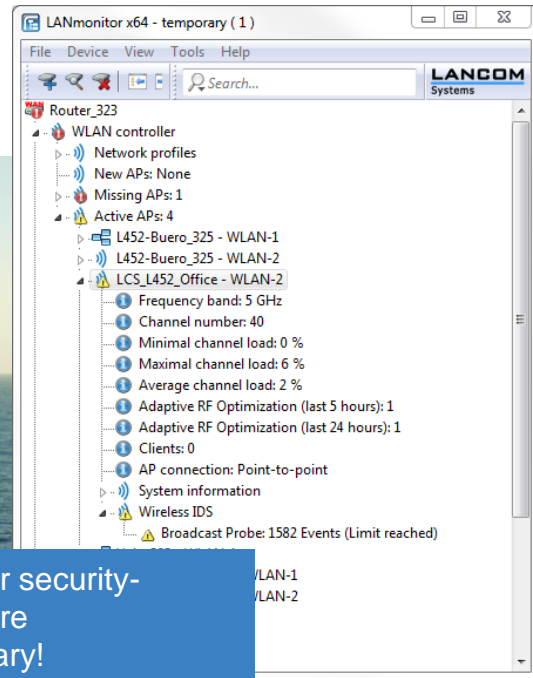
Wireless IDS (Intrusion Detection System)

Early detection of suspicious client behavior

- Detection of attacks or suspicious client behavior in the Wi-Fi infrastructure thanks to the constant surveillance of the radio field
- If an event resembling an attack occurs at a defined frequency, a warning is triggered via e-mail, SYSLOG message, SNMP, or LANmonitor



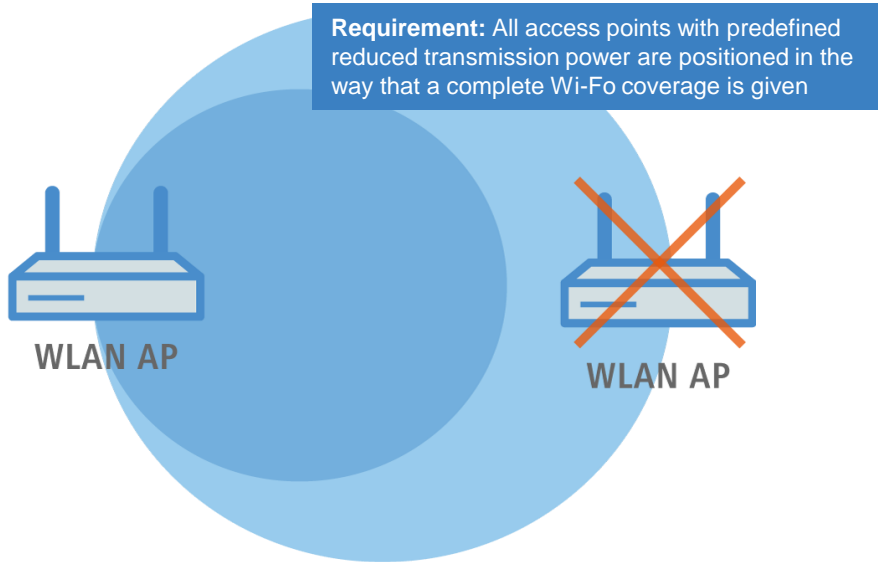
Especially recommended for security-sensitive environments where logging of events is necessary!



Adaptive Transmission Power

Automatic adjustment of the transmission power for Wi-Fi backup scenarios

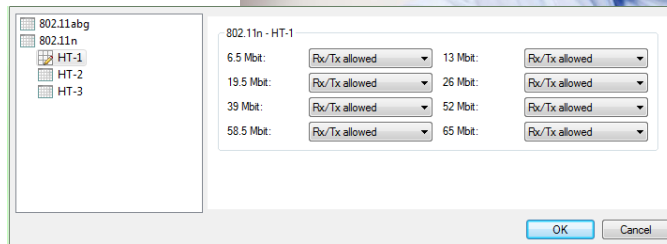
- With the help of actual information about the currently active access points, the transmit powers of all available devices can be adjusted in case of failure
- The other access points close the gaps in the radio field
- If disturbances has ceased the original transmission power reduction is used again



Configurable data rates per SSID

More configuration options – More flexibility

- The predefined data rates for the communication between access points and Wi-Fi clients can now be configured in detail – a real plus in flexibility.
- ➔ Data rates which cannot be used effectively due to environmental conditions can be excluded from operations



Versatile validity of Public Spot access accounts

Definable time units for optimal network utilization

- Vouchers' validity (expiration date) can be set for shorter time periods (days, hours, minutes)
- Booked bandwidth can be displayed on Public Spot vouchers

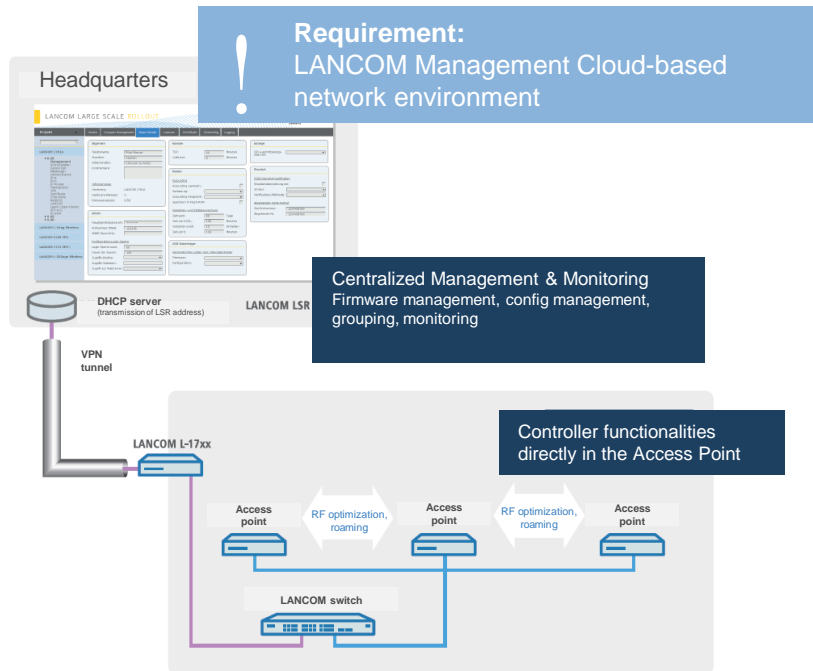
Ideal for scenarios with a high customer frequency and short dwelling times.



Controller-less WLAN management for enterprise scenarios

Zero-touch deployment

- The LANCOM Management Cloud allows:
 - An automatic start-up and configuration allocation ("Zero-touch deployment")
 - Management of LANCOM access points without WLAN controller



LCOS 9.20



The LCOS promise

Available at no charge, the operating system LCOS (LANCOM Operating System) is the in-house closed-source firmware for the entire core portfolio of LANCOM Systems GmbH. LCOS is **developed at the headquarters in a BSI-certified High Security Zone** and receives **software updates with new features and improvements several times** a year. Furthermore, the seal of **quality "IT-Security Made in Germany"** (ITSMG) from an independent organization guarantees **freedom from backdoors**. LCOS is constantly subject to a number of quality tests and therefore offers reliability of the highest degree for professional network infrastructures. Thanks to **future-proof hardware** dimensioning, LANCOM products are designed for a **service life of several years** and the support of future LCOS versions. Even for older devices, which no longer support the newest LCOS version, bug fixes for the latest available firmware are provided on demand. This way, LANCOM offers an **investment protection** that is beyond compare.



Thank you
for your attention.

LANCOM 1781UA-AC