

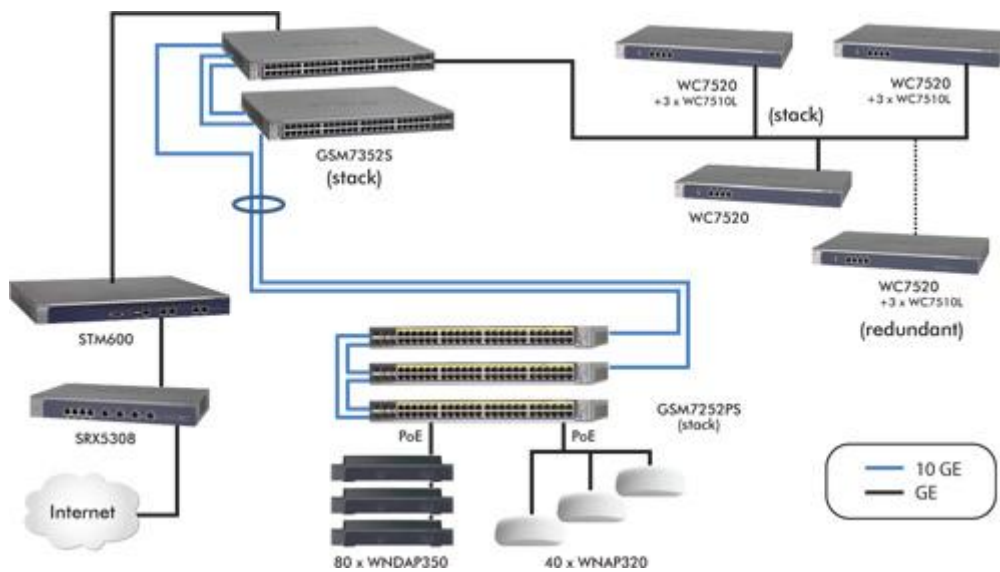


NETGEAR WC7520

PROSAFE 20-AP WIRELESS CONTROLLER

- Reliable, affordable and simple Wireless infrastructure
- Supporting 150 access points and thousands clients
- Seamless roaming and self-healing RF capabilities

Example of Wireless-N configuration with 120 access points (AP) and one redundant controllers.



SYSTEM INFORMATION AND LIMITS

Supported AP Models

- WNDAP360 ProSafe Dual Band 802.11n Wireless Access Point
- WNDAP350 ProSafe Dual Band 802.11n Wireless Access Point
- WNAP320 ProSafe 802.11n Wireless Access Point
- WNAP210 ProSafe 802.11n Wireless Access Point

Supported Modes

- Wireless-A/B/G/N

Maximum AP Supported per Controller

- 20 (default)
- 50 with 3 x Incremental 10-AP License Upgrades (WC7510L)

Maximum Controllers that Can Be Stacked Together

- 3

Maximum AP Supported per Stacked Setup

- 150

Maximum Profile Groups per Controller

- 8
- Each access point belongs to only one profile group

Maximum Security Profiles (SSID) per Profile Group

- 8 per radio (2.4 GHz; 5 GHz)
- 16 with WNDAP350

Maximum Security Profiles (SSID) per Controller

- 128 (assuming WNDAP350/WNDAP360 and 8 security profiles per radio)

Maximum Security Profiles per Network (3 Controllers)

- 512

Maximum Rogue APs Detectable per Controller

- 512

Maximum Floorplans per Controller

- 3 (default)
- Additional floorplans possible with USB local storage (up to a maximum of 18 floorplans)

Number of Captive Portals per Controller

- 1

Maximum Clients per AP

- WNAP210: up to 32 clients; WNAP320: up to 64 clients
- WNDAP350 and WNDAP360: up to 64 clients per radio (128 clients total)

Maximum Clients per Controller

- None other than maximum clients per AP

L2 Mobility

- L2 fast roaming support between the APs

L3 Mobility

- L3 fast roaming support with encrypted tunnelling between the APs and the controller

Maximum VLANs per Controller

- 64 VLANs for SSIDs
- 1 configurable management VLAN

Controller Redundancy

- VRRP-based N+1 redundancy with failover
- 1:1 when one cold redundant Controller and one production Controller are configured to form a Redundancy group
- 1:2 or 1:3 when one cold redundant Controller is added to a Stack of 2 or 3 production Controllers
- Licenses on the redundant controller need - at least - to match those on each protected production controller

LICENSE CONFIGURATIONS

Per Controller: Up to 50 Access Points (AP) with Appropriate Licenses



Per Stack: Up to 150 Access Points (AP) with Appropriate Licenses



CONFIGURATION EXAMPLES - WIRELESS A/B/G/N DEPLOYMENT

Number of Access Points - up to:

20	30	40	50	60	70	80	90	100	110	120	130	140	150
----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----

Number of Wireless Controllers (WC7520)

1	1	1	1	2	2	2	2	2	3	3	3	3	3
---	---	---	---	---	---	---	---	---	---	---	---	---	---

Number of 10-AP Incremental License Upgrades (WC7510L)

0	1	2	3	2	3	4	5	6	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---	---	---	---	---

IP AND VLANS CONFIGURATION

DHCP Server/Relay

- Integrated DHCP server
- Multiple DHCP server/pool can be added for different VLANs (up to 64)

VLANS for the Wireless Controller

- One management VLAN (configurable VLAN ID)

VLANS Access Points / Multiple SSIDs

- 64 VLANs

VLANS Deployment

- The Wireless Controller must have IP connectivity with the access points through the management VLAN. If the Controller and the APs are on different management VLANs, external VLAN routing must allow IP connectivity between the Controller and the APs.

RF PLANNING AND MONITORING

Integrated Deployment Planning

- Hierarchical view of the network: Floor maps upload and floor maps dimensions input
- Automated RF planning algorithm: Computed number of APs required to cover a floor plan

- Theoretical cloud coverage indicated for each AP for positioning assistance on the floor plan

RF Monitoring

- Coverage computing per floor plan
- Alert for any detected coverage holes with mitigation options with neighboring APs
- Rogue AP/blacklisted clients triangulation

RF MANAGEMENT

Automatic Channel Allocation

- Channel automatic distribution to reduce interference
- Auto-channel allocation takes into consideration the AP location, interferences, and neighborhood maps for each AP
- Modifiable list of corporate channels to be used
- Scheduled mode for auto-channel allocation
- Automatic mode available in case of high level of interference

Automatic Power Control

- Optimum transmit power determination based on coverage requirements
- Automatic power control mode available
- Neighborhood scan of RF environment to minimize neighboring AP interference and leakage across floors

Coverage Hole Detection

- Automatic mode
- Down APs or compromised RF environment detection with alerts
- Self healing: Automatic neighboring AP power increase to fill in for coverage losses

Load Balancing

- AP load monitoring and overload prevention
- Client redirection to lightly loaded neighboring APs

Fast Roaming

- Seamless rapid mobility across VLAN and subnets
- Includes 802.11i pre-auth and fast roaming
- Fast roaming support accross L2, and L3 for video, audio and voice over wireless client

QUALITY OF SERVICE

WMM Quality of Service

- WMM (802.11e) prioritizes traffic for both upstream traffic from the stations to the access points (station EDCA parameters) and downstream traffic from the access points to the client stations (AP EDCA parameters)

WMM Queues in Decreasing Order of Priority

- Voice: The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media
- Video: The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue
- Best effort: The medium priority queue with medium delay is given to this queue. Most standard IP application will use this queue
- Background: Low priority queue with high throughput. Applications, such as FTP, which are not time-sensitive but require high throughput can use this queue

WMM Power Save Option

- WMM power save helps conserve battery power in small devices such as phones, laptops, PDAs, and audio players using IEEE® 802.11e mechanisms

Rate Limiting

- Rate limit per SSID set as a percentage of total available bandwidth

WIRELESS SECURITY

Client Authentication Protocols

- Open, WEP, WPA/WPA2-PSK
- 802.11i/WPA/WPA2 Enterprise with standard interface to external AAA/RADIUS Server
- Local ACLs (512 MAC)
- MAC ACLs based on local AAA Server or external Radius Server

Distinct AAA Server per SSID

- Yes

RADIUS Accounting Protocol

- Per Client tracking for:
 - Bytes Tx/Rx
 - Connect/disconnect time
- **LDAP-based Authentication**
 - Standard interface to external LDAP server/Microsoft® Active Directory Server

Integrated AAA Server

- Local database authentication based on WC7520 internal AAA Server

Guest Access

- Integrated captive portal available for client authentication in a security profile
- Password based authentication mode: Local user store available, receptionist assigned user name/password
- External Radius server mode: External RADIUS authentication for the captive portal clients
- Open authentication mode: Guest auto registration with email address
- Extraction of logs of guest activity

Captive Portal

- Configurable portal page, including image files

Rogue Access Points

- Rogue AP definition: AP with radio SSID observed by any of the managed APs and seen transmitting on same L2 wired network
- Detection and mapping of up to 512 rogue APs

WIRELESS NETWORK MONITORING

Monitoring Summary

- Summary of managed access points status, rogue access points detected, wireless stations connected, Wireless Controller information and wireless network usage

Managed Access Points

- AP status for the managed access points and details that includes configuration settings, current wireless settings, current clients and detailed traffic statistics

Rogue Access Points

- Rogue access points reported
- Rogue access points in same channel
- Rogue access points in interfering channels

Wireless Clients

- Clients statistics and details per AP, per SSID, per floor, per location
- Blacklisted clients, roaming clients

Wireless Network Usage

- Network usage statistics display plots of average received/transmitted network traffic per managed access point. Three different plots show Ethernet, Wireless 802.11 b/bg/ng and 802.11 a/na mode traffic separately

Heat Maps

- Live coverage and visualization heat maps
- Location visualization and device tracking

DHCP Leases

- DHCP details for wireless clients

MANAGEMENT

Management Interface

- HTTP, SNMP v1/v2c, telnet, Secure Shell (SSH)

Logging and Reporting

- If available syslog server on the network, the Wireless Controller can send all logs. Logs are also available on the GUI and ready to download (log export file)
- Email alerts for events as per configuration to multiple email addresses

Diagnostics

- Managed access points ping

Maintenance

- Save/restore configuration, restore to factory defaults, admin password change, add user (read-only), firmware upgrade via Web browser for the Wireless Controller and the managed access points

Dual Boot Image

- Supported

SNMP

- SNMP v1/v2c

IEEE AND IETF RFC STANDARDS

Wired IEEE Standards

- IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T
- IEEE 802.1Q VLAN tagging

Wired IEEE Standards

- IEEE 802.11a, 802.11b, 802.11g, 802.11n
- WMM (from 802.11e)

RFC - System Facilities

- RFC 1001 Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods'
- RFC 1002 Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications
- RFC 1155 Management information for TCP/IP networks
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 2131 DHCP
- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP

RFC - Security and AAA

- WPA-PSK, WPA2-PSK
- RFC 1321 MD5 Message – Digest Algorithm
- RFC 1851 Triple DES Algorithm
- RFC 2246 TLS Protocol Version 1.0
- RFC 2404 HMAC-SHA-1-96
- RFC 3280 Internet X.509 PKI Certificate and CRL certificate
- RFC 3377 Lightweight Directory Access Protocol (v3): Technical Specification
- RFC 3565 Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax
- RFC 4346 TLS Protocol version 1.1

IEEE AND IETF RFC STANDARDS

RFC - Management

- SNMP v1, v2c
- RFC 364 syslog
- RFC 854 telnet
- RFC 1156 MIB
- RFC 1157 SNMP
- RFC 1213 MIB II
- RFC 1350 TFTP
- RFC 2616 HTTP
- RFC 3164 The BSD Syslog Protocol
- Enterprise private MIBs

HARDWARE

Gigabit RJ45 Ports LAN

- Switch 4-port 10/100/1000

Flash Memory/RAM

- 8 MB + 2 GB CF/1 GB DDR2

USB Port

- 1 port for USB storage
 - More floor heat maps
 - Extended statistics history

Major Regulatory Compliance

- FCC Class A, CE, WEEE, RoHS

Storage and Operating Temperatures

- Operating temperature 0°-45° C (32°-113° F),
- Storage temperature -20°-70° C (-4°-158° F)

Humidity

- Operation 90% Maximum Relative, Storage 95% Maximum Relative

Electrical Specifications

- 100-240V, AC/50-60Hz, Universal Input, DC 5V/8A (internal power supply)

Dimensions (W x H x D) cm

- 26.1 x 4.3 x 44

Dimensions (W x H x D) in

- 10.3 x 1.7 x 17.3

Weight kb/lb

- 2.912/6.4

System Requirements

- Internet Explorer® 5.0 or higher or Mozilla Firefox® 1.0 or higher

Package Contents

- ProSafe 20-AP Wireless Controller (WC7520), Ethernet cable, power cord, installation guide, resource CD

Warranty

- ProSafe Lifetime Warranty†
- Next business day onsite hardware replacement support, 3 years (included)**

ORDERING INFORMATION - CONTROLLER

North America

- WC7520-100NAS

Europe

- WC7520-100EUS

Asia

- WC7520-100AUS

ORDERING INFORMATION - LICENSES

Incremental 10-AP License Upgrade

- WC7510L-10000S

PROSUPPORT SERVICE PACKS

OnCall 24x7, Category 3

- PMB0333

XPressHW, Category 3

- PRR0333-100 (Australia only)