

DUMPSBOSS.

CompTIA Network+ Exam

CompTIA N10-008

Version Demo

Total Demo Questions: 20

Total Premium Questions: 495

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	88
Topic 2, Exam Pool B	73
Topic 3, Exam Pool C	334
Total	495

QUESTION NO: 1

A network administrator views a network pcap and sees a packet containing the following:

```
community: public  
request-id: 13438  
get-response 1.3.6.1.2.1.1.3.0 Value:206901150
```

Which of the following are the BEST ways for the administrator to secure this type of traffic? (Select TWO).

- A. Migrate the network to IPv6.
- B. Implement 802.1 X authentication
- C. Set a private community string
- D. Use SNMPv3.
Utilize IPsec tunneling.
- E. Incorporate SSL encryption

ANSWER: C D

Explanation:

The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

QUESTION NO: 2

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

- A. Fiber
- B. Leased line
- C. Satellite
- D. Metro optical

ANSWER: C

Explanation:

If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

QUESTION NO: 3

Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

- A. DaaS
- B. IaaS
- C. PaaS
- D. SaaS

ANSWER: B

QUESTION NO: 4

Users are reporting poor wireless performance in some areas of an industrial plant. The wireless controller is measuring a low EIRP value compared to the recommendations noted on the most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

- A. AP transmit power
- B. Channel utilization
- C. Signal loss
- D. Update ARP tables
- E. Antenna gain
- F. AP association time

ANSWER: A E

Explanation:

In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain.

QUESTION NO: 5

A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

- A. BYOD policy
- B. NDA
- C. SLA
- D. MOU

ANSWER: B

Explanation:

NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References: <https://www.adobe.com/sign/esignature-resources/sign-nda.html>

QUESTION NO: 6

Which of the following can be used to decrease latency during periods of high utilization of a firewall?

- A. Hot site
- B. NIC teaming
- C. HA pair
- D. VRRP

ANSWER: B

Explanation:

NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes:

<https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=-1&pg=what+is+nic+teaming+used+for&sc=10-28&qsn=&sk=&cvid=13882A9A9B584D8099F4ABCAD034E821&ghsh=0&ghacc=0&ghpl=>

QUESTION NO: 7

Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers. However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

- A. They used the wrong type of fiber transceiver.

- B. Incorrect TX/RX polarity exists on the link
- C. The connection has duplexing configuration issues.
- D. Halogen light fixtures are causing interference.
- E. One of the technicians installed a loopback adapter.
- F. The RSSI was not strong enough on the link

ANSWER: A B

QUESTION NO: 8

A network engineer receives the following when connecting to a switch to configure a port:

```
telnet 10.1.200.1
Connecting to 10.1.200.1...Could not open connection to the host, on port 23: Connect failed.
```

Which of the following is the MOST likely cause for the failure?

- A. The network engineer is using the wrong protocol
- B. The network engineer does not have permission to configure the device
- C. SNMP has been secured with an ACL
- D. The switchport the engineer is trying to configure is down

ANSWER: D

QUESTION NO: 9

A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion, zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

- A. CPU usage
- B. Memory
- C. Temperature
- D. Bandwidth
- E. Latency
- F. Jitter

ANSWER: A B

QUESTION NO: 10

Switch 3 was recently added to an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from their workstations. Following are the port configurations for the switch stack in question:

Switch 1:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Active	Active	Active

Switch 2:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Shut down	Active	Active

Switch 3:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	80	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Shut down	Shut down	Shut down	Active

Which of the following should be configured to resolve the issue? (Select TWO).

- A. Enable the printer ports on Switch 3.
- B. Reconfigure the duplex settings on the printer ports on Switch 3.
- C. Reconfigure the VLAN on an printer ports to VLAN 20.
- D. Enable all ports that are shut down on me stack.
- E. Reconfigure me VLAN on the printer ports on Switch 3.
- F. Enable wireless APs on Switch 3.

ANSWER: A E

QUESTION NO: 11

During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

- A. 22
- B. 23

- C. 69
- D. 443
- E. 587
- F. 8080

ANSWER: B C

QUESTION NO: 12

A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

- A. Data loss prevention policy
- B. BYOD policy
- C. Acceptable use policy
- D. Non-disclosure agreement
- E. Disaster recovery plan
- F. Physical network diagram

ANSWER: B F

QUESTION NO: 13

An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

- A. Load balancing
- B. Multipathing
- C. NIC teaming
- D. Warm site

ANSWER: A

Explanation:

Load balancing is a technique that can be used to provide fault tolerance and high performance while appearing as one URL to users. It is achieved by distributing the workload across multiple servers, which are usually located in different geographical locations. This allows for high performance and fault tolerance, as if one server fails, the other will take its place. Additionally, the multiple servers appear as one URL to the users, eliminating the need for the users to switch between servers.

QUESTION NO: 14 - (SIMULATION)

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum

The Access Points should be configured to only support TKIP clients at a maximum speed

INSTRUCTIONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



192.168.1.2
Speed: Auto
Duplex: Auto

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name: AP1

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: Yes No

Wireless

Mode:

Channel:

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name: AP2

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: Yes No

Wireless

Mode:
 B
 G

Channel:
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: /

Gateway: 192.168.1.1

SSID:

SSID Broadcast: Yes No

Wireless

Mode:
 B
 G

Channel:
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase:

ANSWER: See explanation below.

Explanation:

On the first exhibit, the layout should be as follows

The screenshot displays the 'AP1 Configuration' web interface. The browser address bar shows 'https://ap1.setup.do'. The interface is divided into four main sections:

- Basic Configuration:**
 - Access Point Name: AP1
 - IP Address: 192.168.1.32
 - Gateway: 192.168.1.1
 - SSID: CorpNet
 - SSID Broadcast: Yes No
- Wireless:**
 - Mode: B
 - Channel: 3
- Wired:**
 - Speed: Auto 100 1000
 - Duplex: Auto Half Full
- Security Configuration:**
 - Security Settings: None WEP WPA WPA2 WPA2 - Enterprise
 - Key or Passphrase: S3cr3tl

AP1 Configuration

https://ap1.setup.do

IP Address: 192.168.1.32 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: Yes No

Wireless

Mode: B

Channel: 3

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase: S3cr3tl

AP1 Configuration

https://ap1.setup.do

IP Address: 192.168.1.3 / 27
Gateway: 192.168.1.1
SSID: CorpNet
SSID Broadcast: Yes No

Wireless

Mode: G
Channel: 3

Wired

Speed: Auto 100 1000
Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise
Key or Passphrase: S3cr3t!

Reset to Default Save Close

Exhibit 2 as follows

Access Point Name AP2

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name: AP2

IP Address: 192.168.1.64 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: Yes No

Wireless

Mode: B

Channel: 6

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

Security Configuration

Reset to Default Save Close

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase: S3cr3tl

The screenshot displays the 'AP2 Configuration' web interface. At the top, there is a blue header with the title 'AP2 Configuration' and a close button. Below the header is a browser address bar showing 'https://ap2.setup.do'. The main configuration area is divided into several sections:

- Basic Network Settings:** IP Address (192.168.1.4), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes selected).
- Wireless Settings:** Mode (G) and Channel (6).
- Wired Settings:** Speed (Auto selected) and Duplex (Auto selected).
- Security Configuration:** Security Settings (WPA selected) and Key or Passphrase (S3cr3t!).

At the bottom of the interface, there are three buttons: 'Reset to Default', 'Save', and 'Close'.

Exhibit 3 as follows

Access Point Name AP3

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: Yes No

Wireless

Mode: B

Channel: 9

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

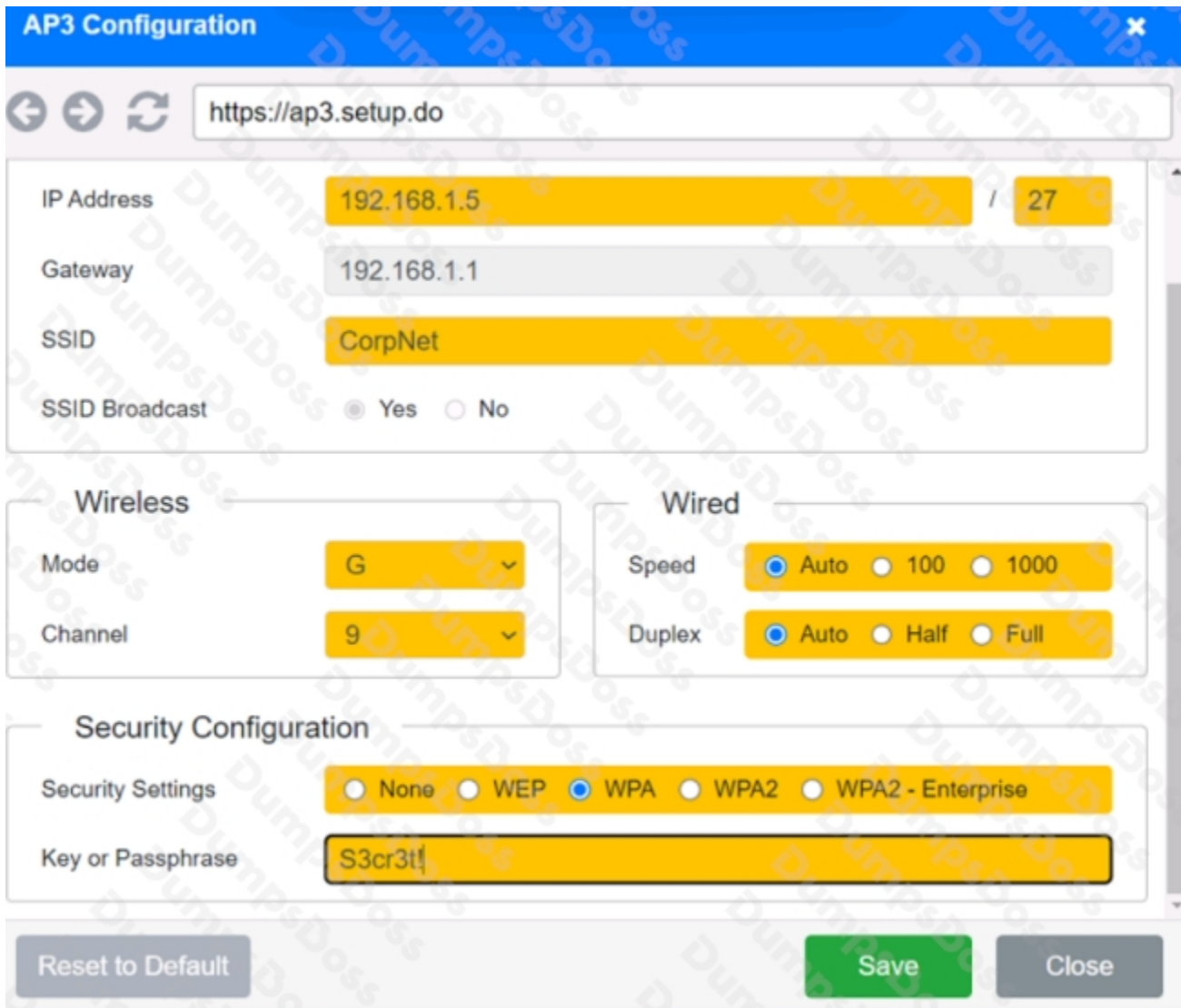
Security Configuration

Reset to Default Save Close

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase: S3cr3t!



The screenshot shows the AP3 Configuration web interface. At the top, there is a blue header with the title "AP3 Configuration" and a close button. Below the header is a navigation bar with back, forward, and refresh icons, and a URL bar containing "https://ap3.setup.do". The main configuration area is divided into several sections:

- Basic Configuration:** IP Address (192.168.1.5), Gateway (192.168.1.1), SSID (CorpNet), and SSID Broadcast (Yes selected).
- Wireless Configuration:** Mode (G), Channel (9).
- Wired Configuration:** Speed (Auto selected), Duplex (Auto selected).
- Security Configuration:** Security Settings (WPA selected), Key or Passphrase (S3cr3t!).

At the bottom, there are three buttons: "Reset to Default", "Save", and "Close".

QUESTION NO: 15

A network administrator responds to a support ticket that was submitted by a customer who is having issues connecting to a website inside of the company network. The administrator verifies that the customer could not connect to a website using a URL. Which of the following troubleshooting steps would be BEST for the administrator to take?

- A. Check for certificate issues
- B. Contact the ISP
- C. Attempt to connect to the site via IP address
- D. Check the NTP configuration.

ANSWER: C**Explanation:**

The best option for the administrator to take would be to attempt to connect to the site via IP address. This will help to determine if the issue is related to the website's DNS address or if the site itself is not accessible. Checking for certificate issues may be necessary, but this should be done after the administrator has attempted to connect to the site via IP address. Contacting the ISP is unnecessary since the issue is related to the website inside of the company network, and checking the NTP configuration is not relevant to this issue.

When a customer is having issues connecting to a website using a URL, one of the first troubleshooting steps a network administrator should take is attempting to connect to the site using the IP address of the website. This will help to determine if the issue is related to a DNS resolution problem or a connectivity problem. If the administrator is able to connect to the website using the IP address, then the issue may be related to a DNS problem. However, if the administrator is still unable to connect, then the issue may be related to a connectivity problem. In either case, further troubleshooting steps will be necessary. Checking for certificate issues or NTP configuration, and contacting the ISP would not be the BEST initial steps in this scenario.

QUESTION NO: 16

Which of the following issues are present with RIPv2? (Select TWO).

- A. Route poisoning
- B. Time to converge
- C. Scalability
- D. Unicast
- E. Adjacent neighbors
- F. Maximum transmission unit

ANSWER: B C

Explanation:

The disadvantages of RIP (Routing Information Protocol) include the following.

---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.

---The more well-known problem of the 15 hop limitation in which data must travel

---Convergence time is terrible for information propagation in a network

---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel

---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'.

RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

QUESTION NO: 17

An employee reports to a network administrator that internet access is not working. Which of the following should the administrator do FIRST?

- A. Establish a theory of probable cause.
- B. Identify symptoms.
- C. Determine if anything has changed.
- D. Ask the user to restart the computer.

ANSWER: C

Explanation:

When a user reports that internet access is not working, it is important to first determine if there have been any recent changes to the network or the user's computer that could have caused the issue. This could include changes to the network configuration, the installation of new software or hardware, or other events that could have impacted the user's ability to access the internet. By determining if anything has changed, the administrator can narrow down the possible causes of the issue and focus on addressing the most likely cause.

QUESTION NO: 18

A network administrator is looking at switch features and is unsure whether to purchase a model with PoE. Which of the following devices that commonly utilize PoE should the administrator consider? (Select TWO)

- A. VoIP phones
- B. Cameras
- C. Printers
- D. Cable modems
- E. Laptops
- F. UPSs

ANSWER: A B

Explanation:

Power over Ethernet (PoE) is a technology that allows network-connected devices to receive power over the same Ethernet cables that are used for data transfer. PoE is commonly used to power devices such as VoIP phones and cameras, making it an ideal choice for network administrators looking for a cost-effective solution. PoE is not typically used for other devices such as printers, cable modems, laptops, and UPSs.

QUESTION NO: 19

A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

- A. Ensure an implicit permit rule is enabled
- B. Configure the log settings on the firewalls to the central syslog server
- C. Update the firewalls with current firmware and software
- D. Use the same complex passwords on all firewalls

ANSWER: C

Explanation:

Updating the firewalls with current firmware and software is an important step to ensure all the firewalls are hardened successfully, as it can fix any known vulnerabilities or bugs and provide new features or enhancements. Enabling an implicit permit rule is not a good practice for firewall hardening, as it can allow unwanted traffic to pass through the firewall. Configuring the log settings on the firewalls to the central syslog server is a good practice for monitoring and auditing purposes, but it does not harden the firewalls themselves. Using the same complex passwords on all firewalls is not a good practice for password security, as it can increase the risk of compromise if one firewall is breached. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.3 Given a scenario, implement network hardening techniques.

QUESTION NO: 20

An administrator would like to allow Windows clients from outside the office to access workstations without using third-party software. Which of the following access methods would meet this requirement?

- A. Remote desktop gateway
- B. Split tunnel
- C. Site-to-site VPN
- D. VNC

ANSWER: A

Explanation:

To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.

To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.

Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.