Chapter 6

Remote Access

Tran Thanh Dien, PhD

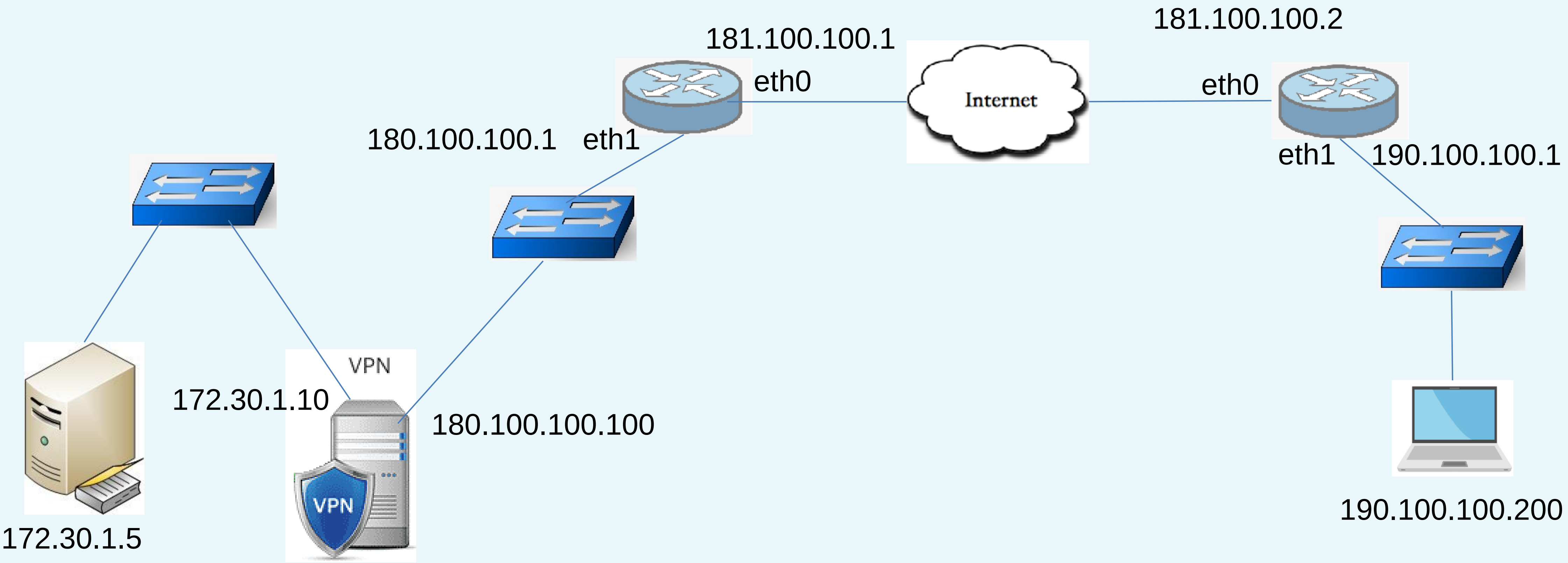
August, 2022

Content

- Remote Access Options
- VPN
- DirectAccess – automatic VPN!
- The truth about DirectAccess and IPv6
- Prerequisites for DirectAccess
- Remote Access Management Console
- DirectAccess versus VPN
- Web Application Proxy

Mobile Workforce

- Most companies and employees have the expectation that they will be able to get their work done from wherever they happen to be



Remote Access

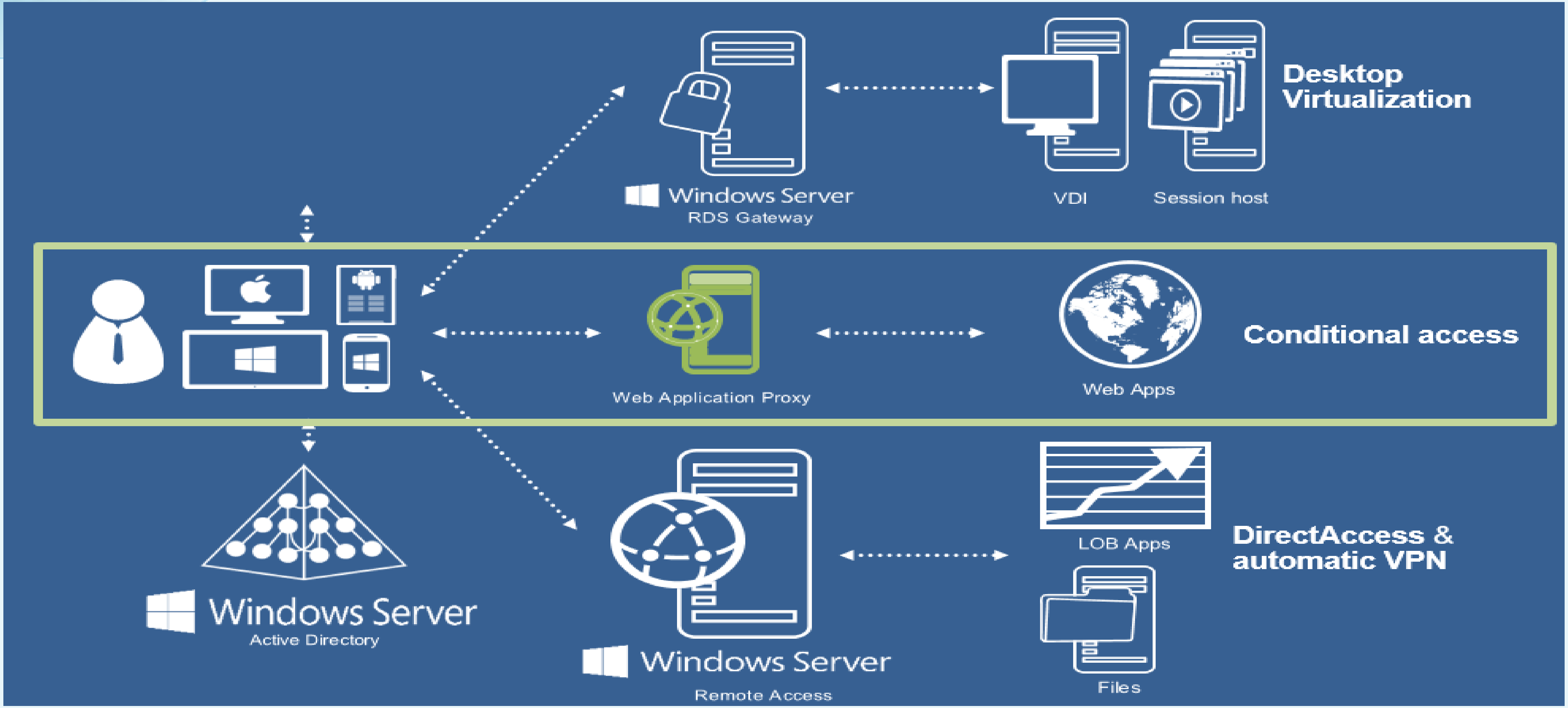
Remote Access

When to use remote access

- Do you allow users to connect to your network resources remotely? If so, how?
- What are your business requirements for using remote access?

Remote Access

Remote access Options



Remote Access

Remote access Options

- Historically relied on third-party tools to connect remote users to the network, such as traditional and SSL VPN
- Windows Server 2016: Two flavors of remote access available:
  - Direct Access (DA): for domain-joined client computers (Windows 7, 8, and 10);
  - VPN for the rest

Remote Access

Remote access Options

- Direct Access (DA):
  - kind of automatic VPN.
  - the user don’t needs to do anything in order to be connected to work.
  - The computer are connected automatically to the corporate network
- The DA machines are typically the company-owned corporate assets
- The client machines must be *joined to the company’s domain*
- The DA configuration settings are brought down to the client through a **GPO**

Remote Access

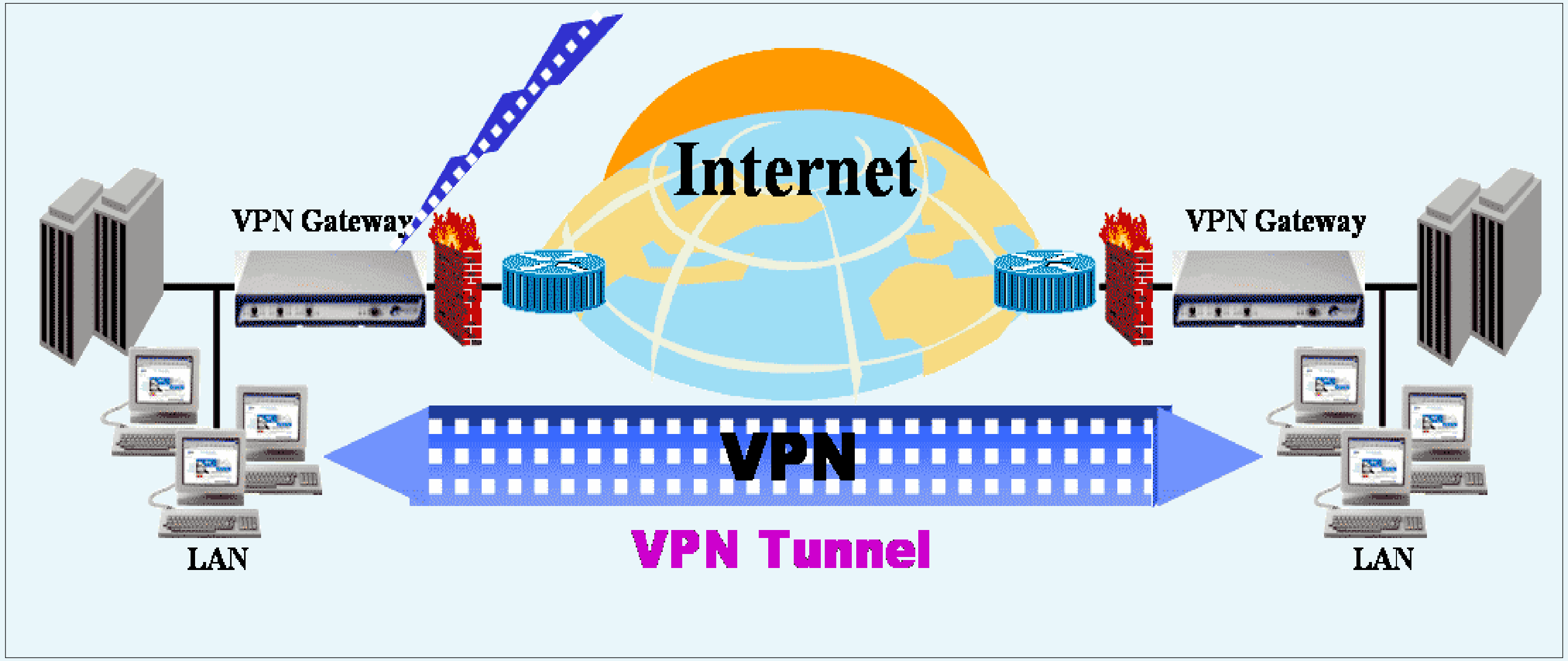
Remote access Options

- VPN is used for
  - down-level clients such as Windows XP
  - non-domain-joined Windows 7/8/10
  - home and personal devices that want to access the network.
- All regular protocols available such as PPTP, L2TP, and SSTP,
- It can even work to connect devices such as smartphones and tablets to the corporate network.

Virtual private network (VPN)

VPN

VPN: a network uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network



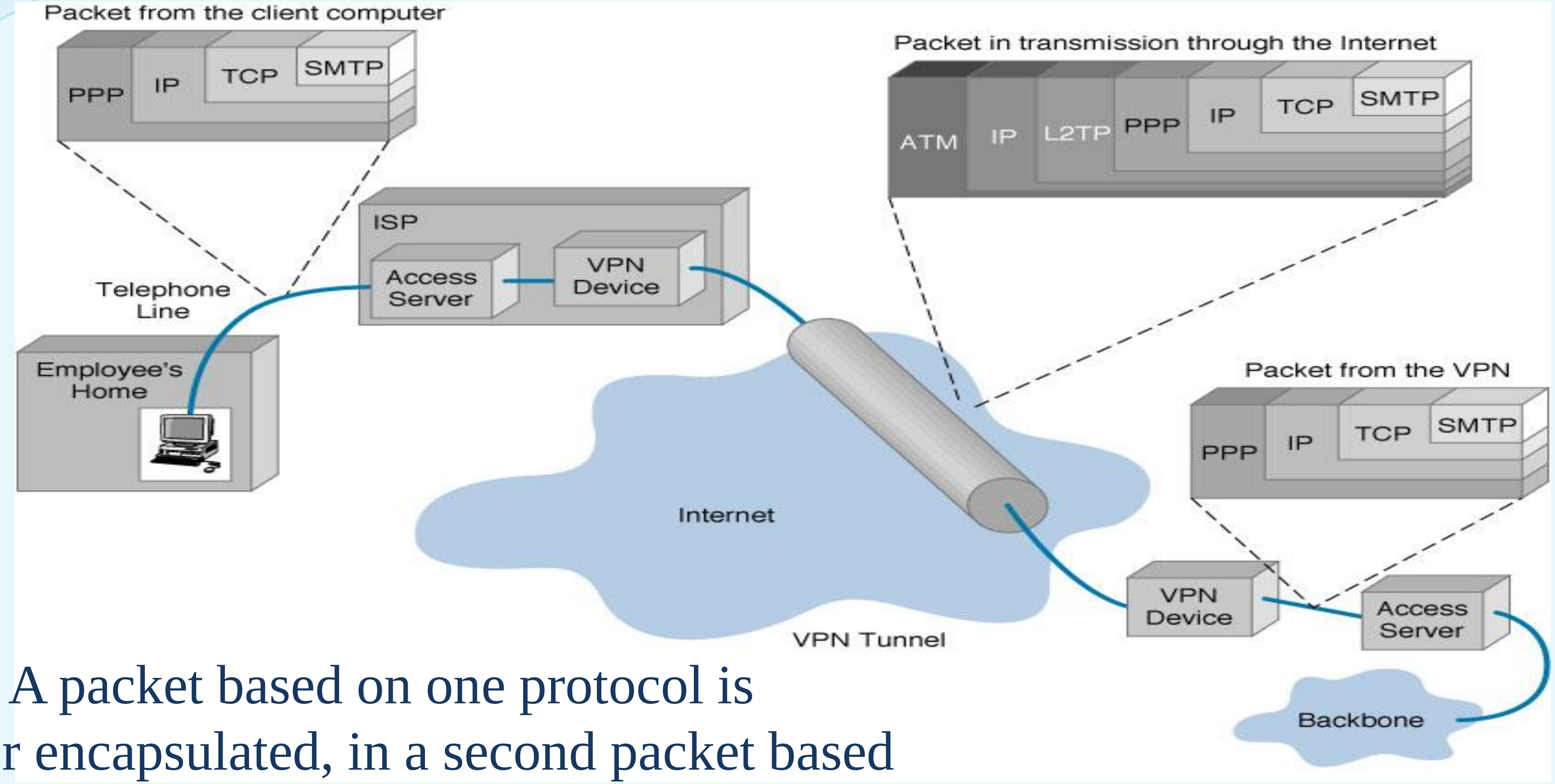
VPN

Four Critical Functions

- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

VPN

Tunneling Protocols



Tunneling: A packet based on one protocol is wrapped, or encapsulated, in a second packet based on a different protocol

VPN

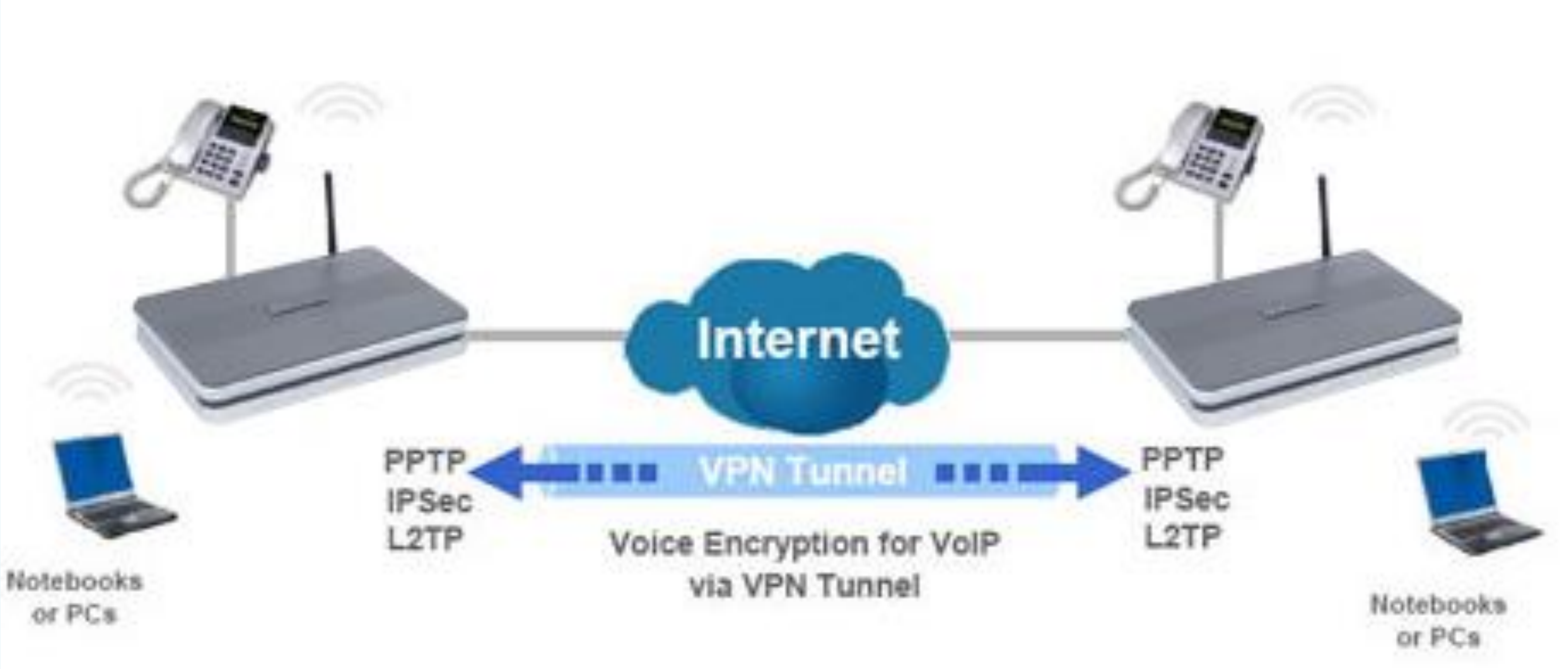
Tunneling Protocols

- Tunneling:
  - a virtual point-to-point connection made through a public network
  - the main ingredient to a VPN
  - used by VPN to creates its connection
- Packets encapsulated and possibly encrypted
- Two types of end points:
  - Remote Access
  - Site-to-Site

VPN

Tunneling Protocols

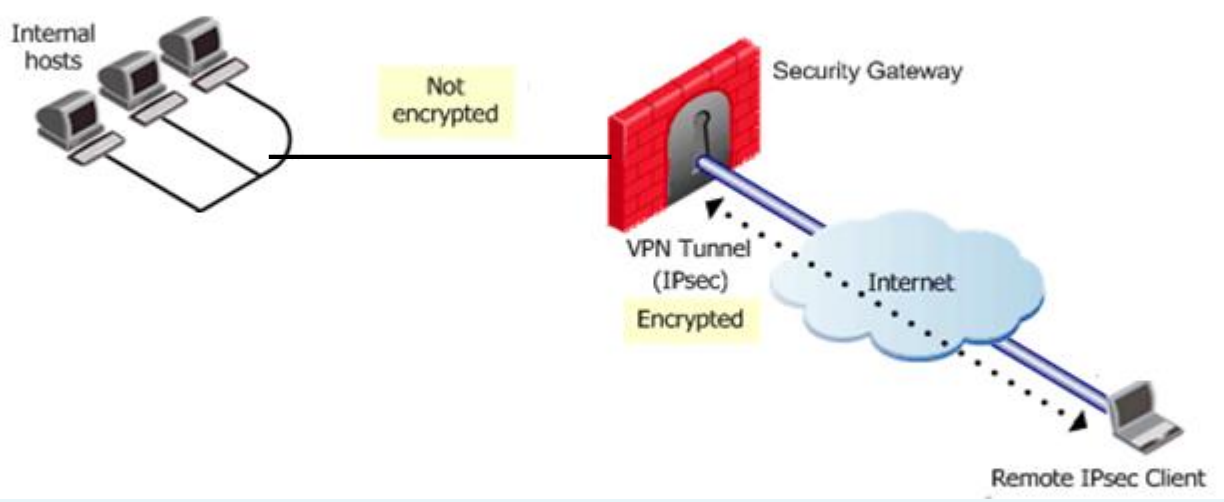
- Three main tunneling protocols used in VPN connections:
  - IPSec -- Internet Protocol Security
  - PPTP -- Point-to-Point Tunneling Protocol
  - L2TP -- Layer 2 Tunneling Protocol

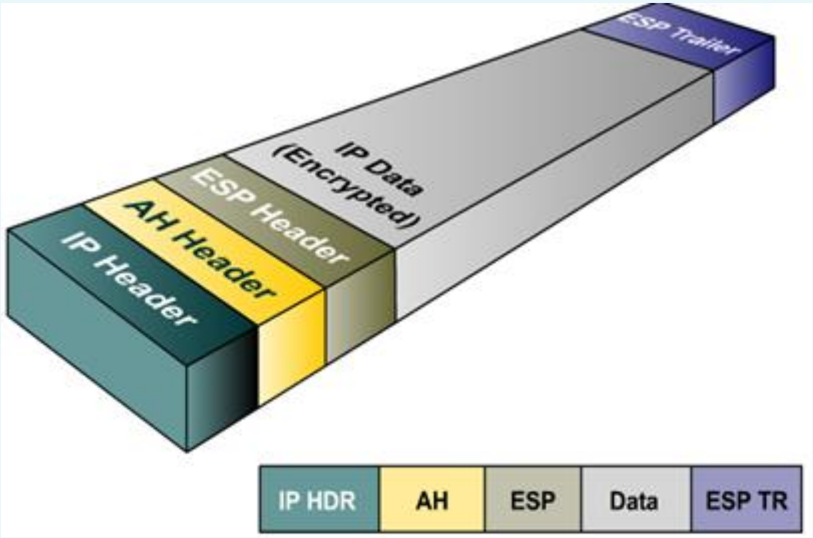


VPN

Internet Protocol Security (IPSec)

- Provides a method of setting up a secure channel for protected data exchange between two devices.

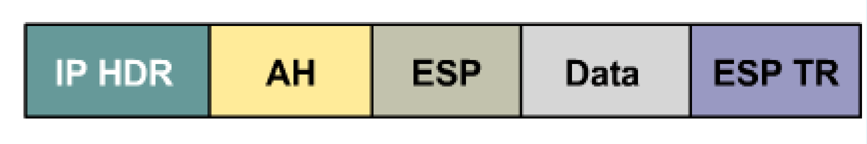


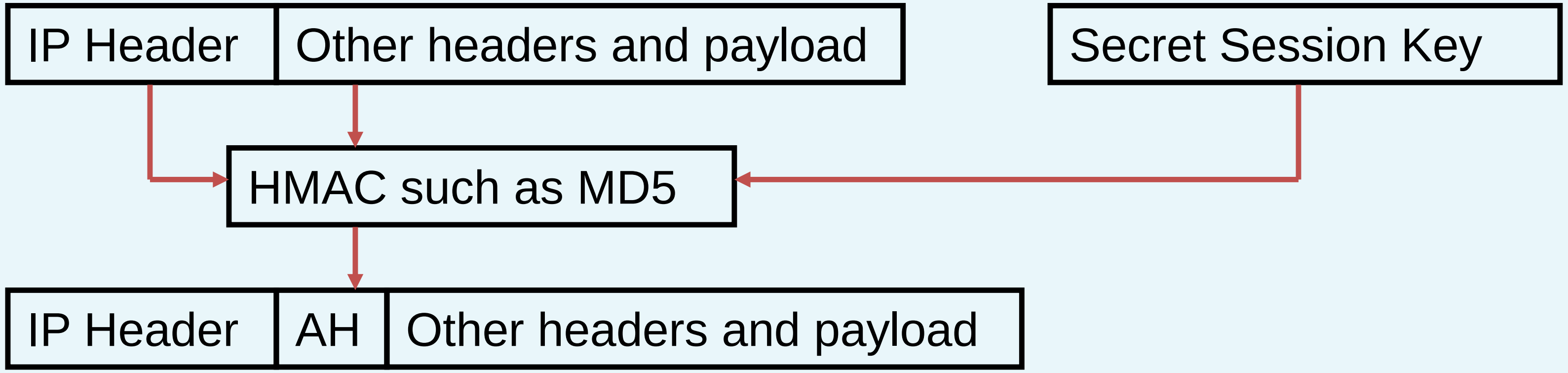


- IPSec consists of two basic security protocols:
  - Authentication (AH): the authentication
  - Encapsulating Security Payload (ESP): provides source authentication, confidentiality, and message integrity

VPN

IPSec

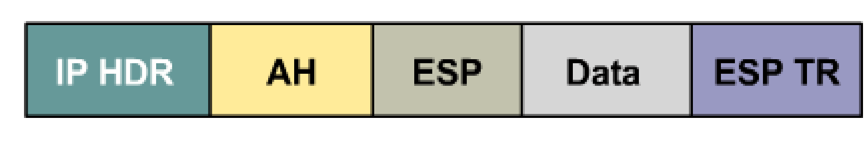




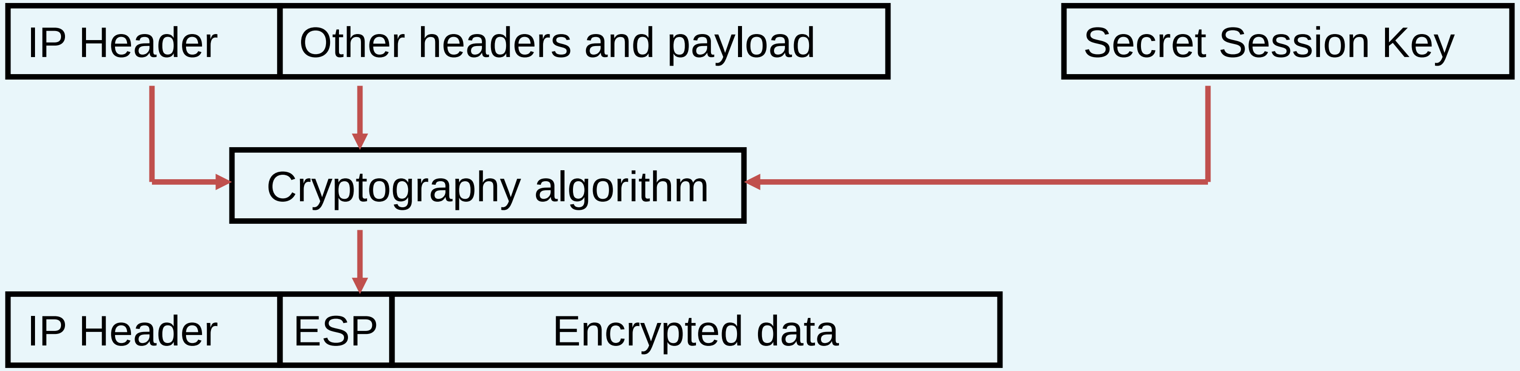
- AH provides data integrity and authentication
- Entire IP packet put through one-way hash (also called an HMAC)
- TTL must be “zeroized” to give a “standard header”
- AH may be applied alone, in combination with the IP ESP.

VPN

IPSec



IP HDR	AH	ESP	Data	ESP TR

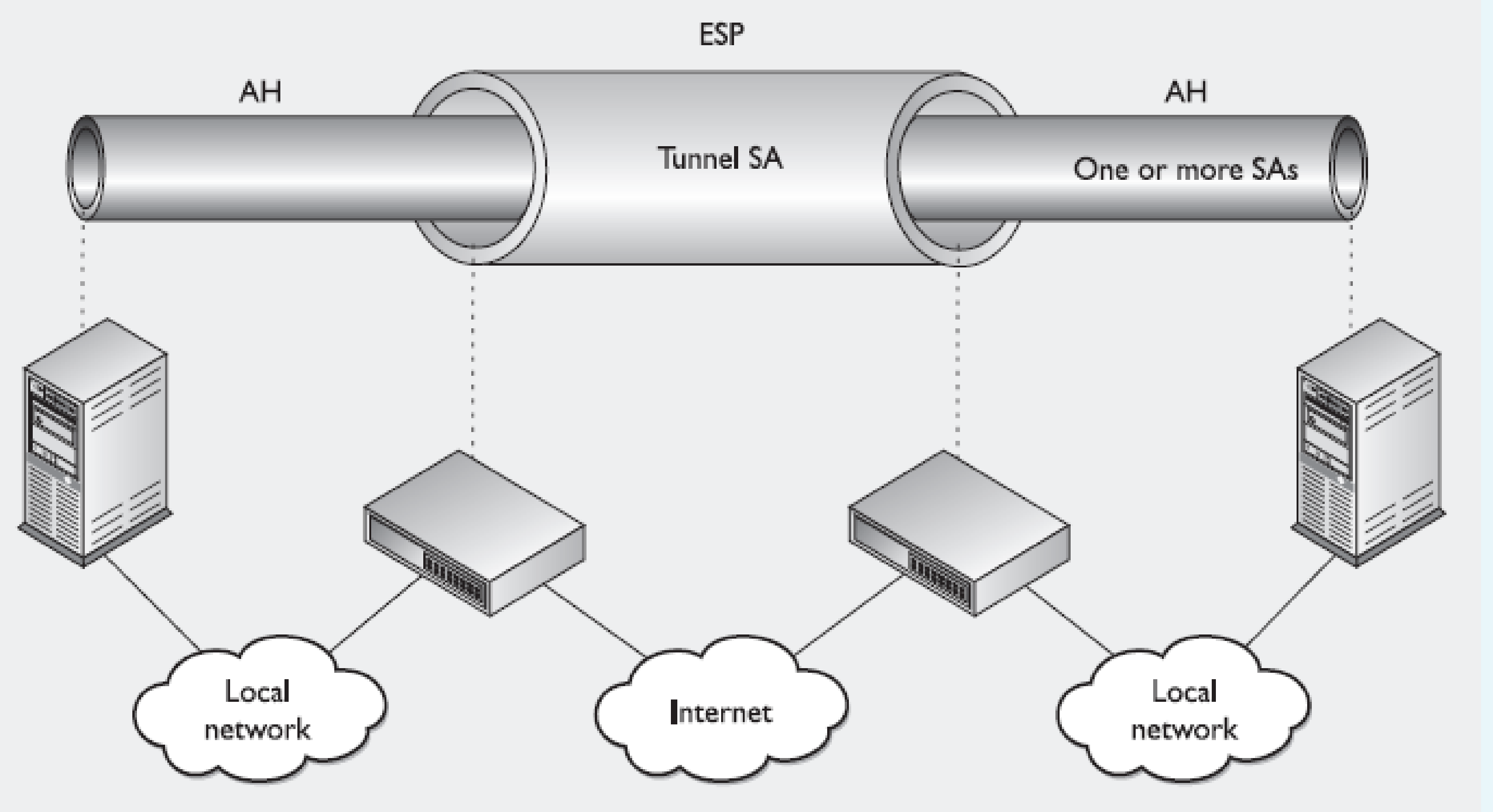


- ESP is primarily used to provide payload encryption. It also provides authentication and integrity
- Different algorithms for payload encryption, including: DES; 3DES; AES

VPN

IPSec

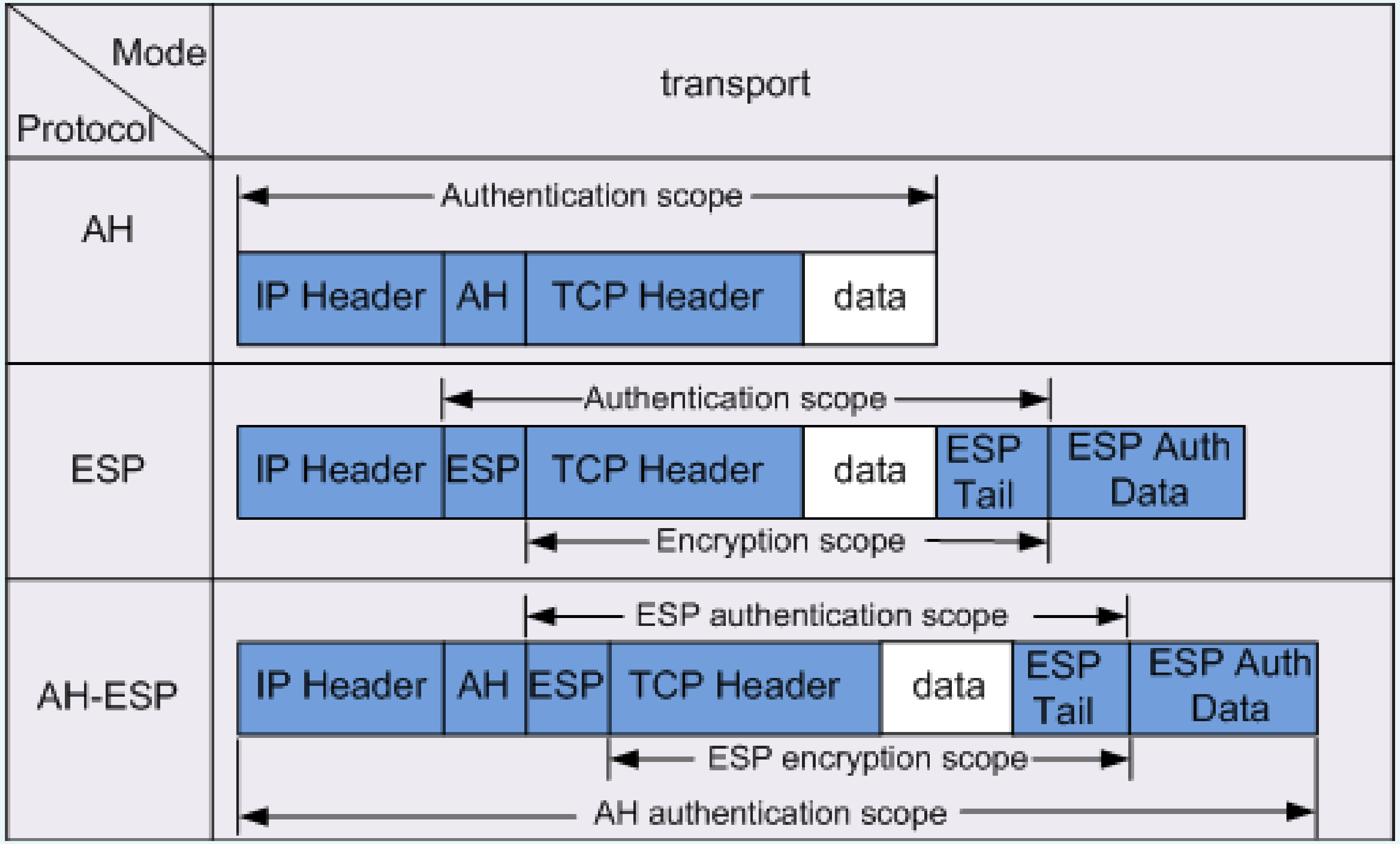
- Two modes:
  - Transport mode: payload of the message is protected
  - Tunnel mode: payload, routing and header information are protected



VPN

IPSec: Transport mode

- Not change the IP packet header
- Source and destination addresses of IPsec tunnel must be the source and destination addresses in the IP packet header.

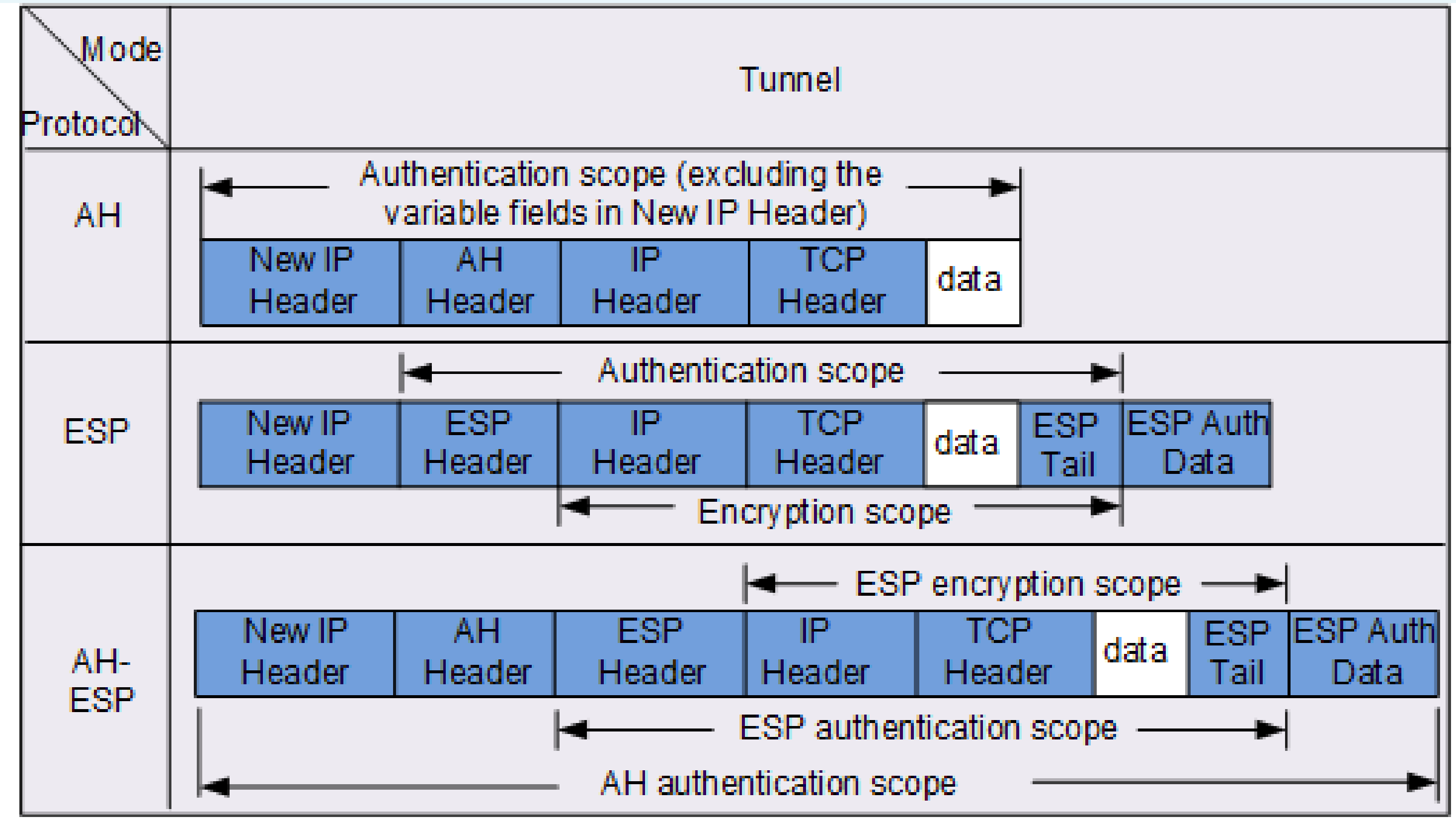


- applicable only to communications between hosts.

VPN

IPSec: Tunnel mode

- The original IP packet is encapsulated into a new IP packet
- Once the receiving end receives the packet:
  - ✓ Removes the new IP header
  - ✓ Decrypts original header

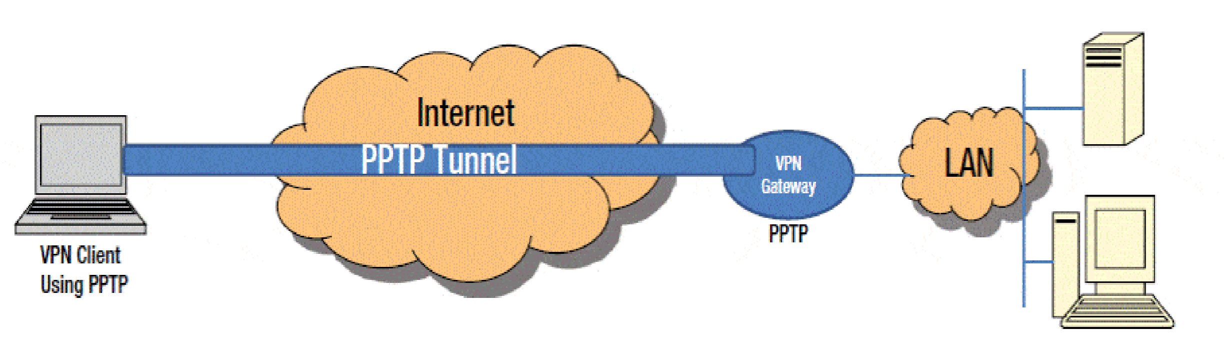


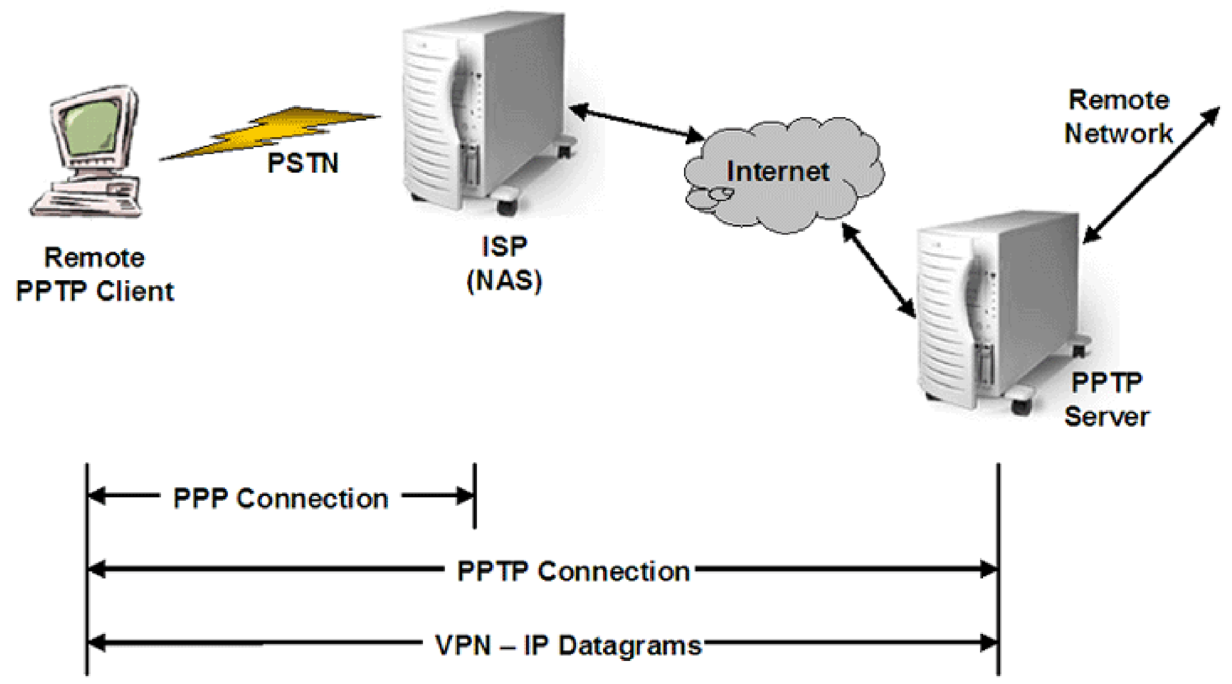
Mode / Protocol	Tunnel
AH	Authentication scope (excluding the variable fields in New IP Header) New IP Header | AH Header | IP Header | TCP Header | data
ESP	Authentication scope New IP Header | ESP Header | IP Header | TCP Header | data | ESP Tail | ESP Auth Data Encryption scope
AH-ESP	ESP encryption scope New IP Header | AH Header | ESP Header | IP Header | TCP Header | data | ESP Tail | ESP Auth Data ESP authentication scope AH authentication scope

- Mainly applicable to communications between VPN gateways or between a host and a VPN gateway.

VPN

Point-to-Point Tunneling Protocol (PPTP)



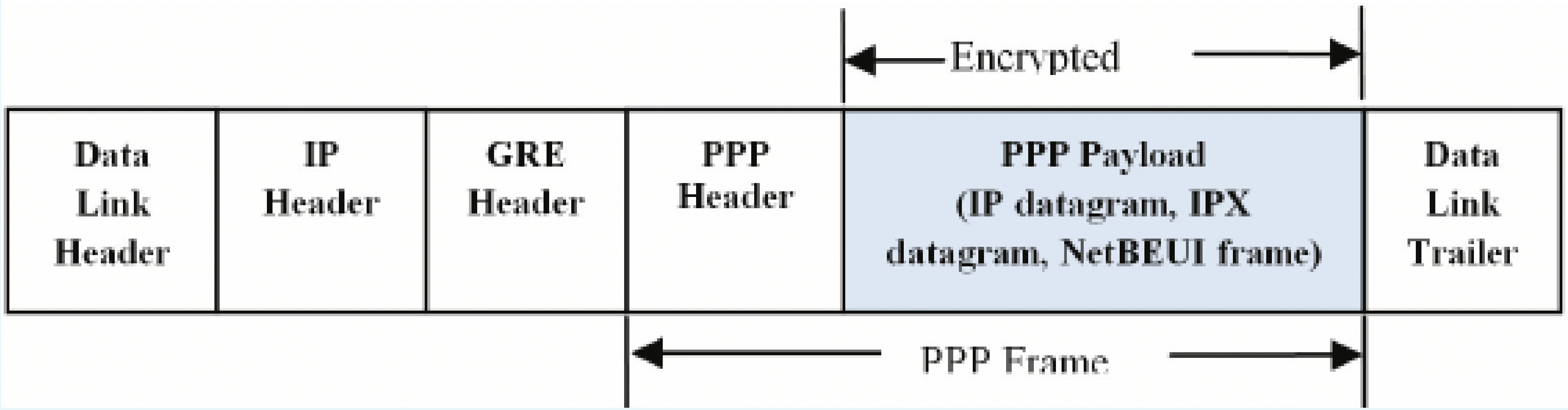


- PPTP is a Microsoft protocol to allow remote users to set up a PPP connection to a local ISP and then create a secure VPN to their destination
- Designed for client/server connectivity
- Single point-to-point connection between two computers
- Works at the data link layer
- Transmits over IP networks only

VPN

PPTP

- In PPTP, the PPP payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MS-CHAP or EAP-TLS.



Data Link Header	IP Header	GRE Header	PPP Header	PPP Payload (IP datagram, IPX datagram, NetBEUI frame)	Data Link Trailer

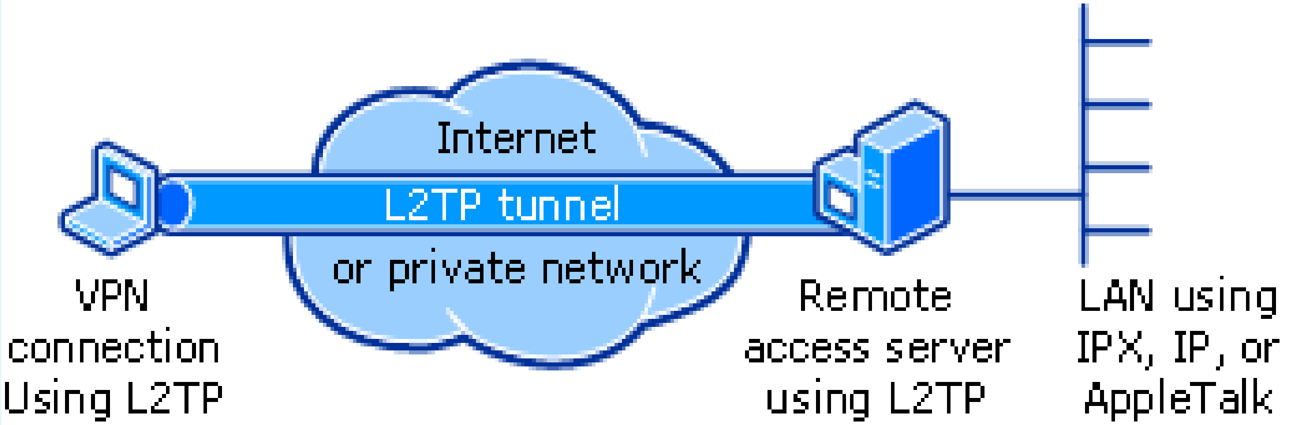
- The keys used in encrypting this data are generated during the authentication process between the user and the authentication server.
- only work over IP networks

VPN

Layer 2 Tunneling Protocol (L2TP)

- L2TP provides the functionality of PPTP, but work over networks other than just IP

- L2TP does not provide any encryption or authentication services.
- It needs to be combined with IPSec if encryption and authentication services are required.


Internet
L2TP tunnel
or private network
VPN connection Using L2TP
Remote access server using L2TP
LAN using IPX, IP, or AppleTalk

VPN

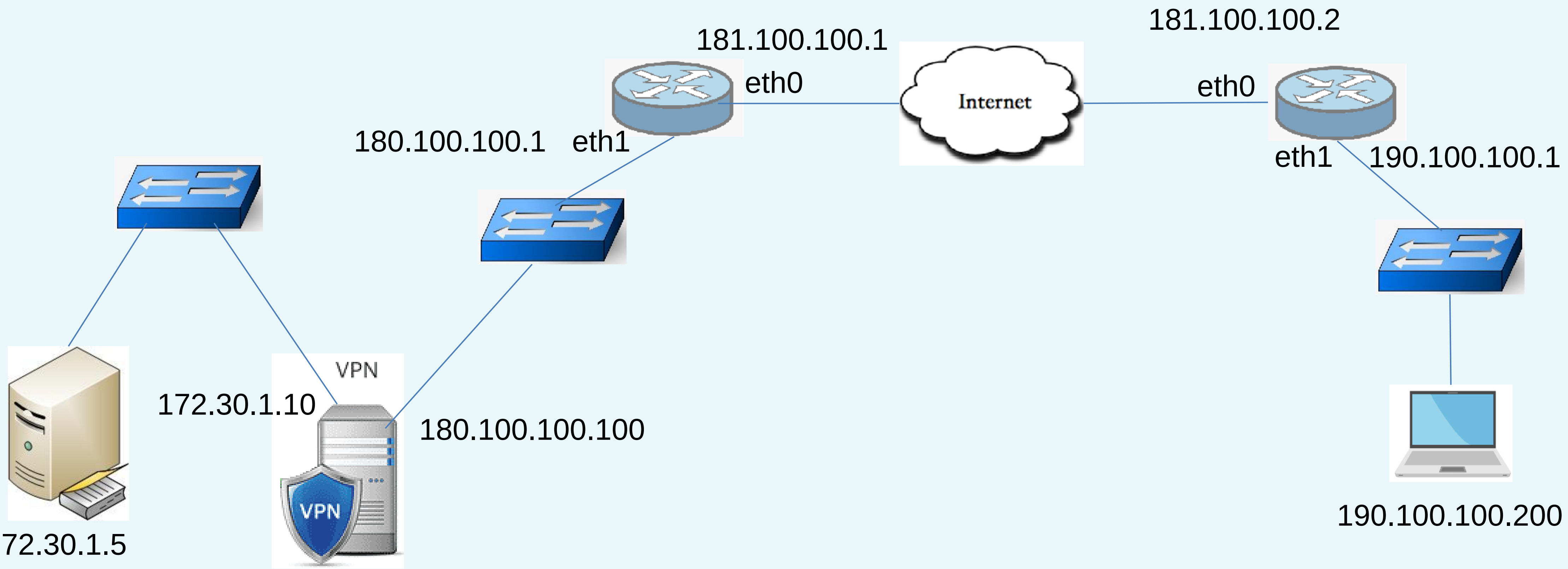
L2TP

- Layer 2 Tunneling Protocol (L2TP)
  - Sets up a single point-to-point connection between two computers
  - Works at the data link layer
  - Transmits over multiple types of networks, not just IP
  - Combined with IPSec for security

VPN

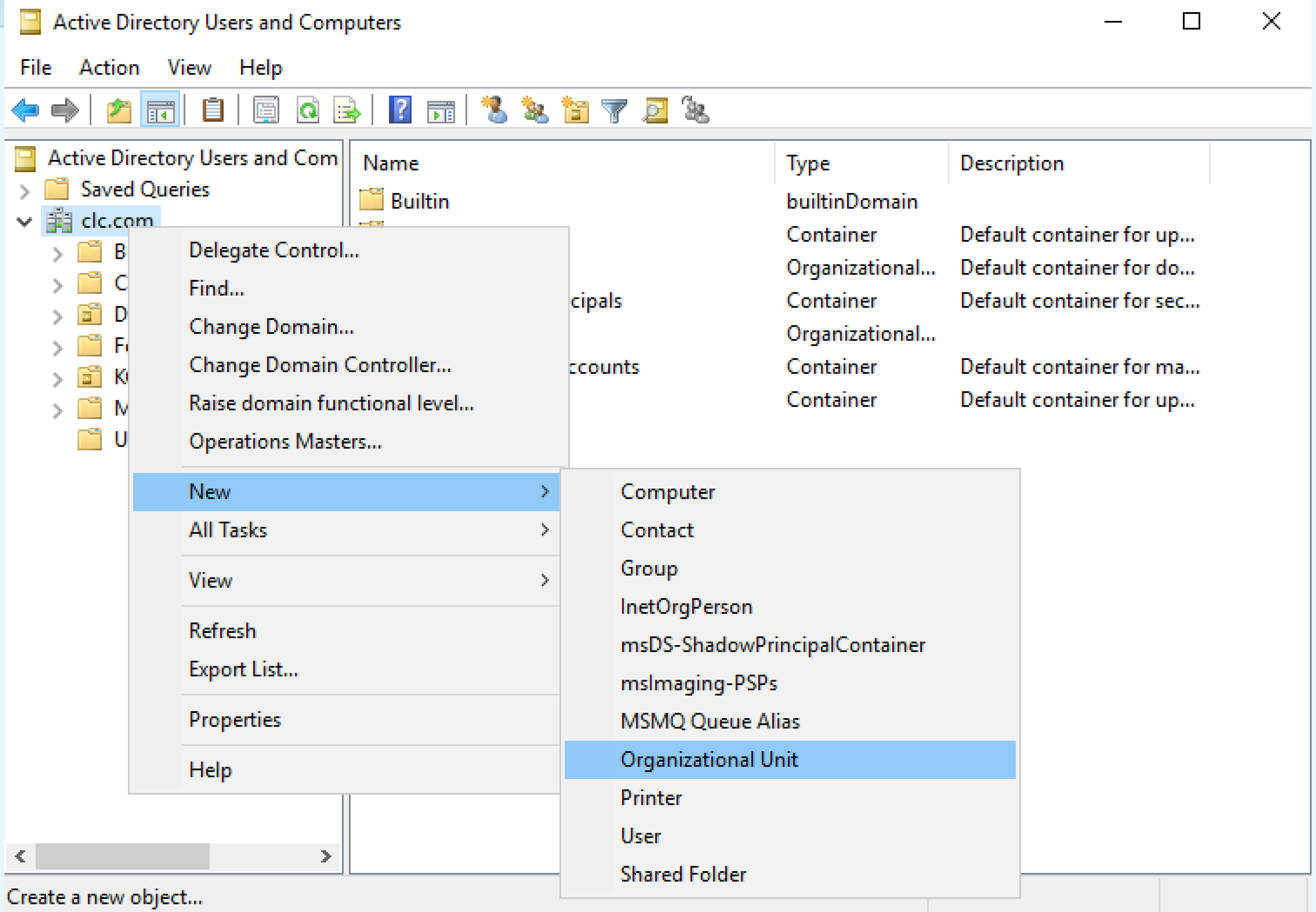
Install and Configure

- VPN Server Requires 2 NIC: 1 for internal network (LAN) and 1 for external network (Internet)

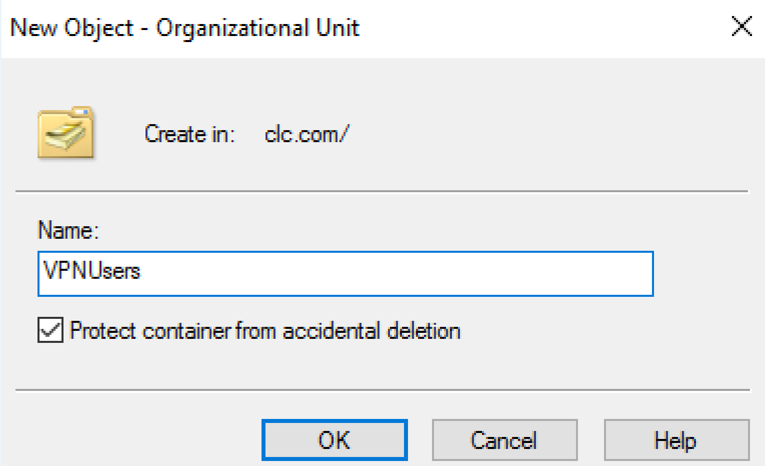


VPN

Install and Configure: Creating OU & Users for VPN



Name	Type	Description
Builtin	builtinDomain	
	Container	Default container for up...
	Organizational...	Default container for do...
cipals	Container	Default container for sec...
	Organizational...	
ccounts	Container	Default container for ma...
	Container	Default container for up...



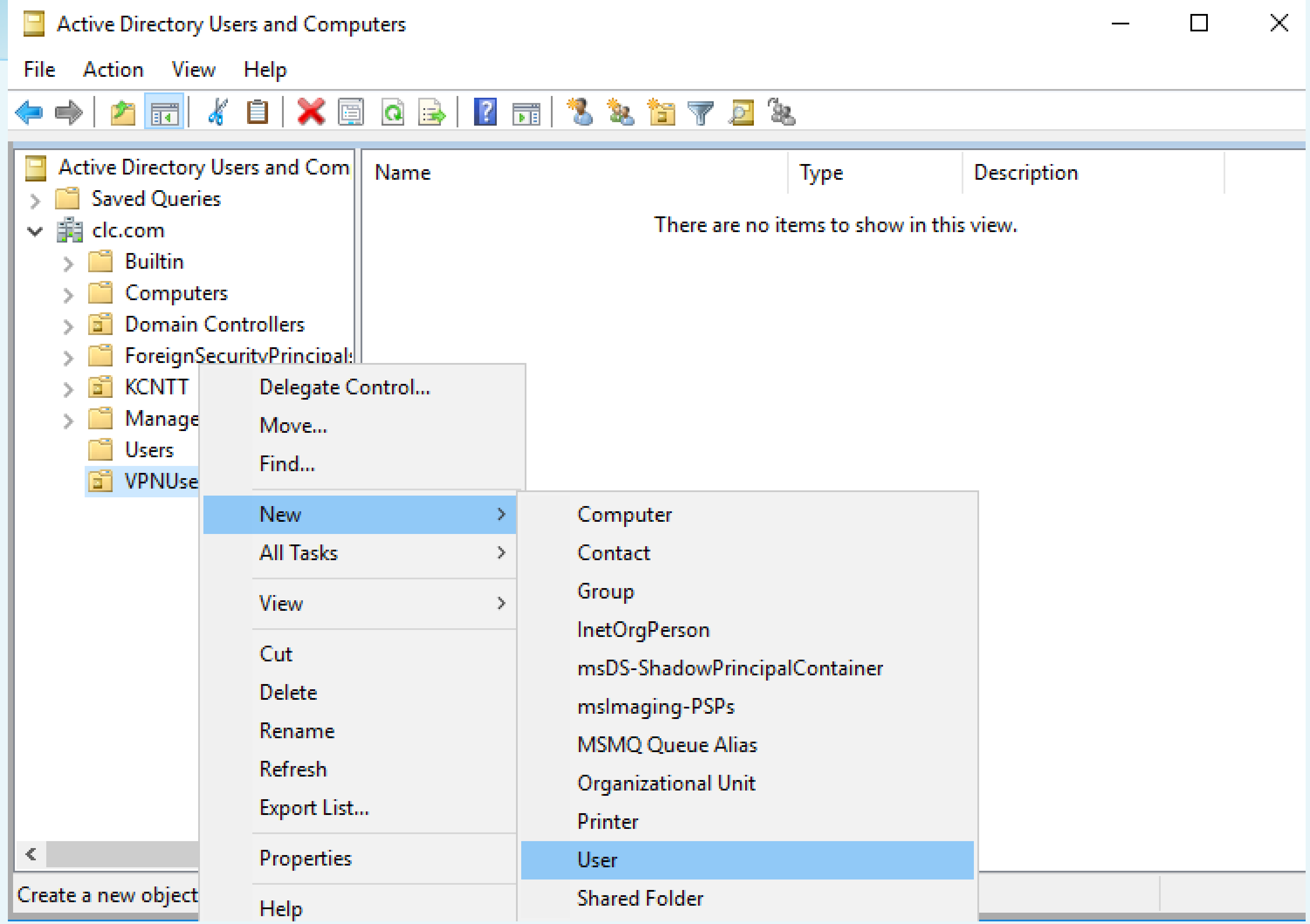
Create in: clc.com/

Name: VPNUsers

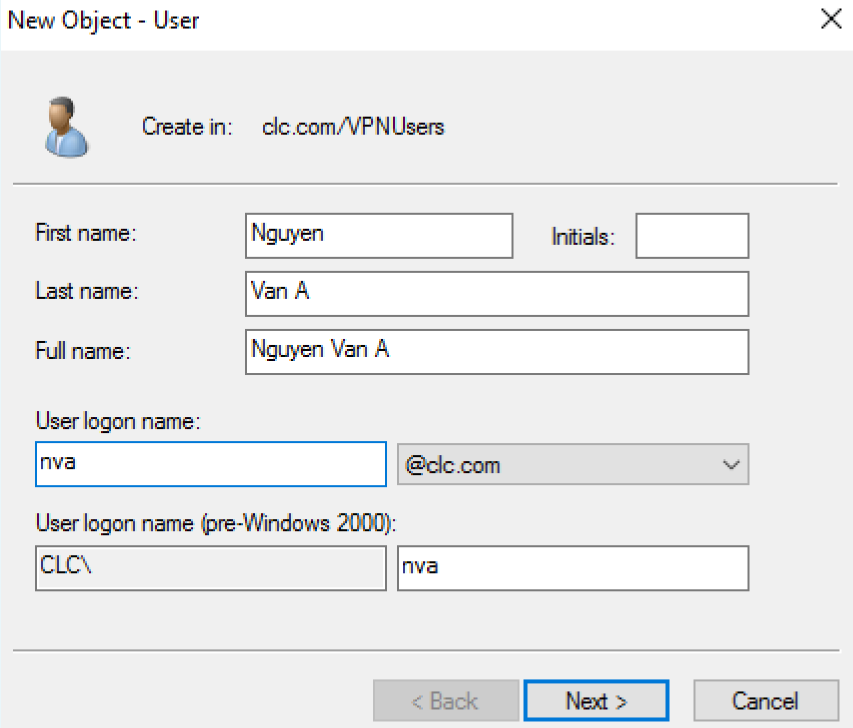
☑ Protect container from accidental deletion

VPN

Install and Configure: Creating OU & Users for VPN



There are no items to show in this view.


New Object - User

Create in: clc.com/VPNUsers

First name: Nguyen

Initials:

Last name: Van A

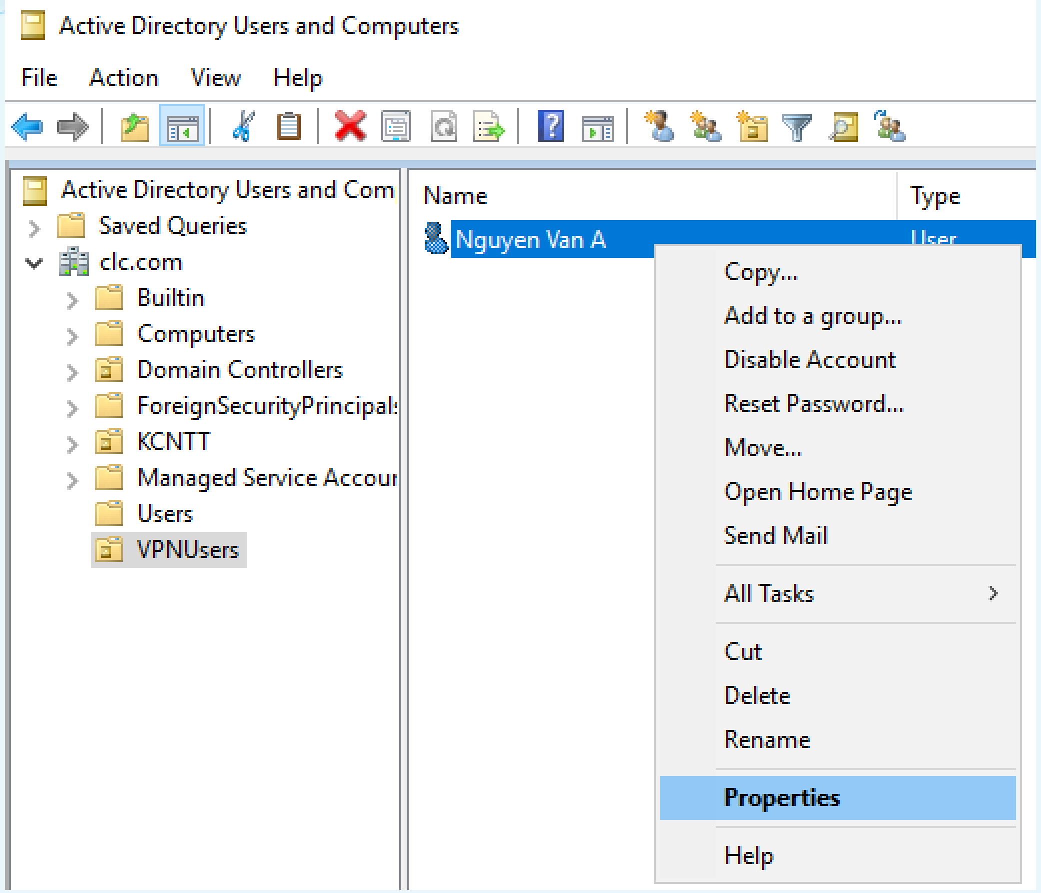
Full name: Nguyen Van A

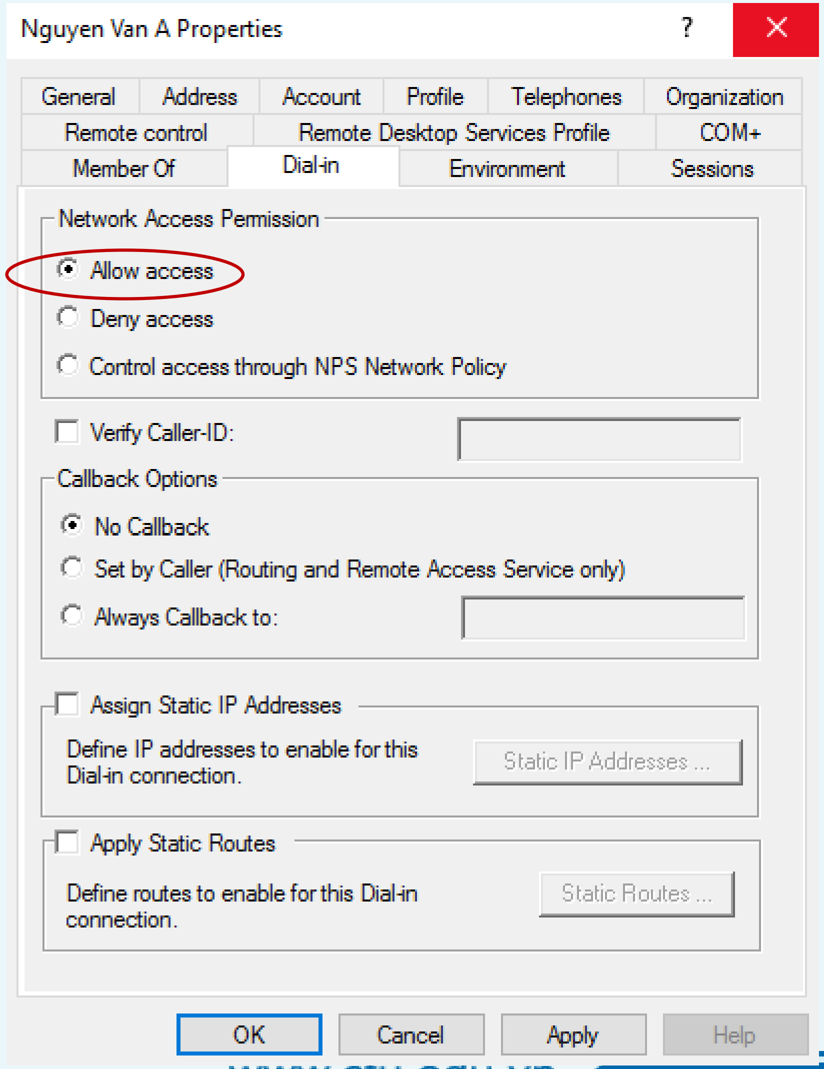
User logon name: nva @clc.com

User logon name (pre-Windows 2000): CLC\ nva

VPN

Install and Configure: Creating OU & Users for VPN




Nguyen Van A Properties

General | Address | Account | Profile | Telephones | Organization | Remote control | Remote Desktop Services Profile | COM+ | Member Of | Dial-in | Environment | Sessions

Network Access Permission

● Allow access

○ Deny access

○ Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

Static IP Addresses ...

□ Apply Static Routes

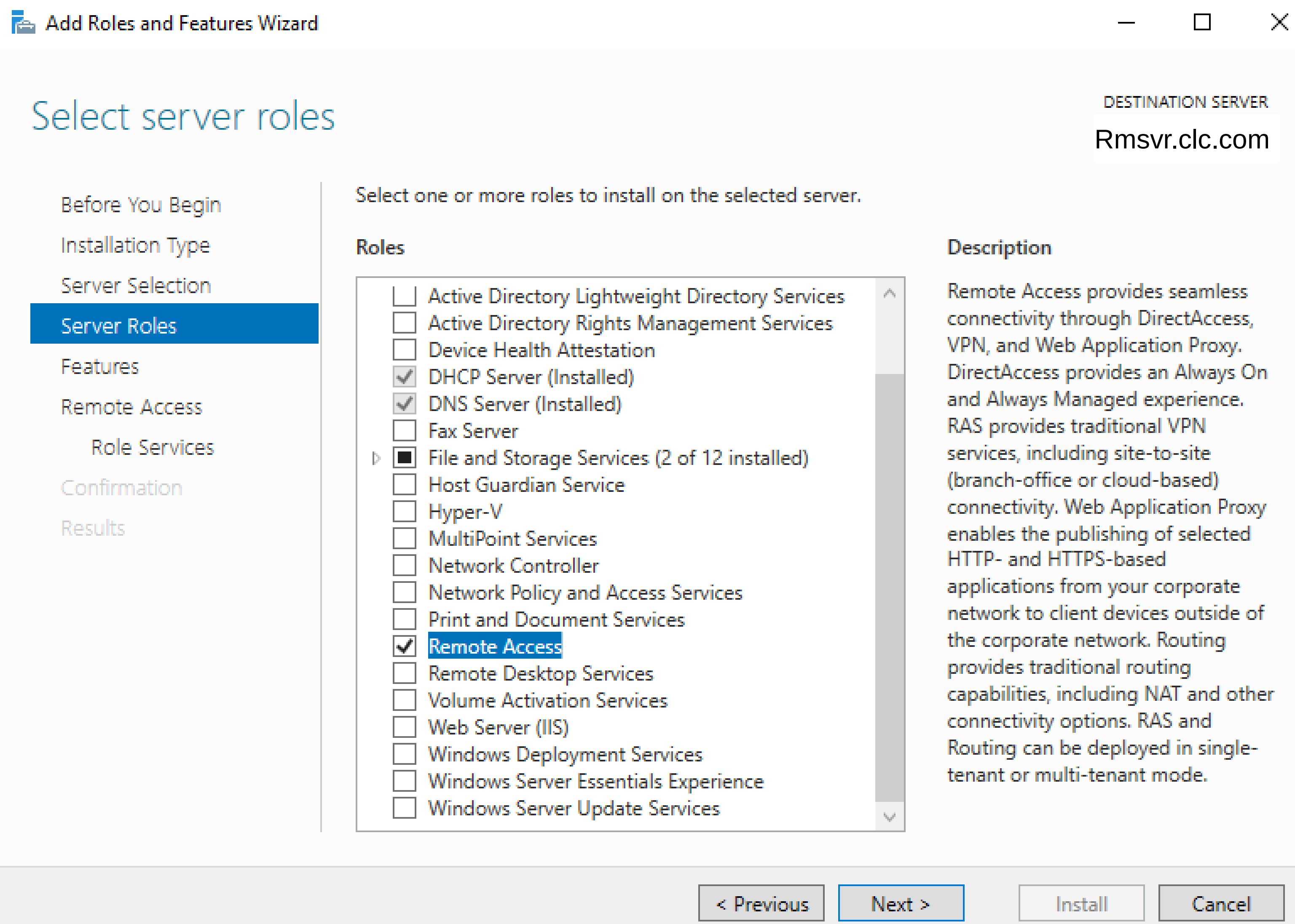
Define routes to enable for this Dial-in connection.

Static Routes ...

OK | Cancel | Apply | Help

VPN

Install and Configure: Add Remote Access Role



Select server roles

DESTINATION SERVER
Rmsvr.clc.com

Select one or more roles to install on the selected server.

Roles

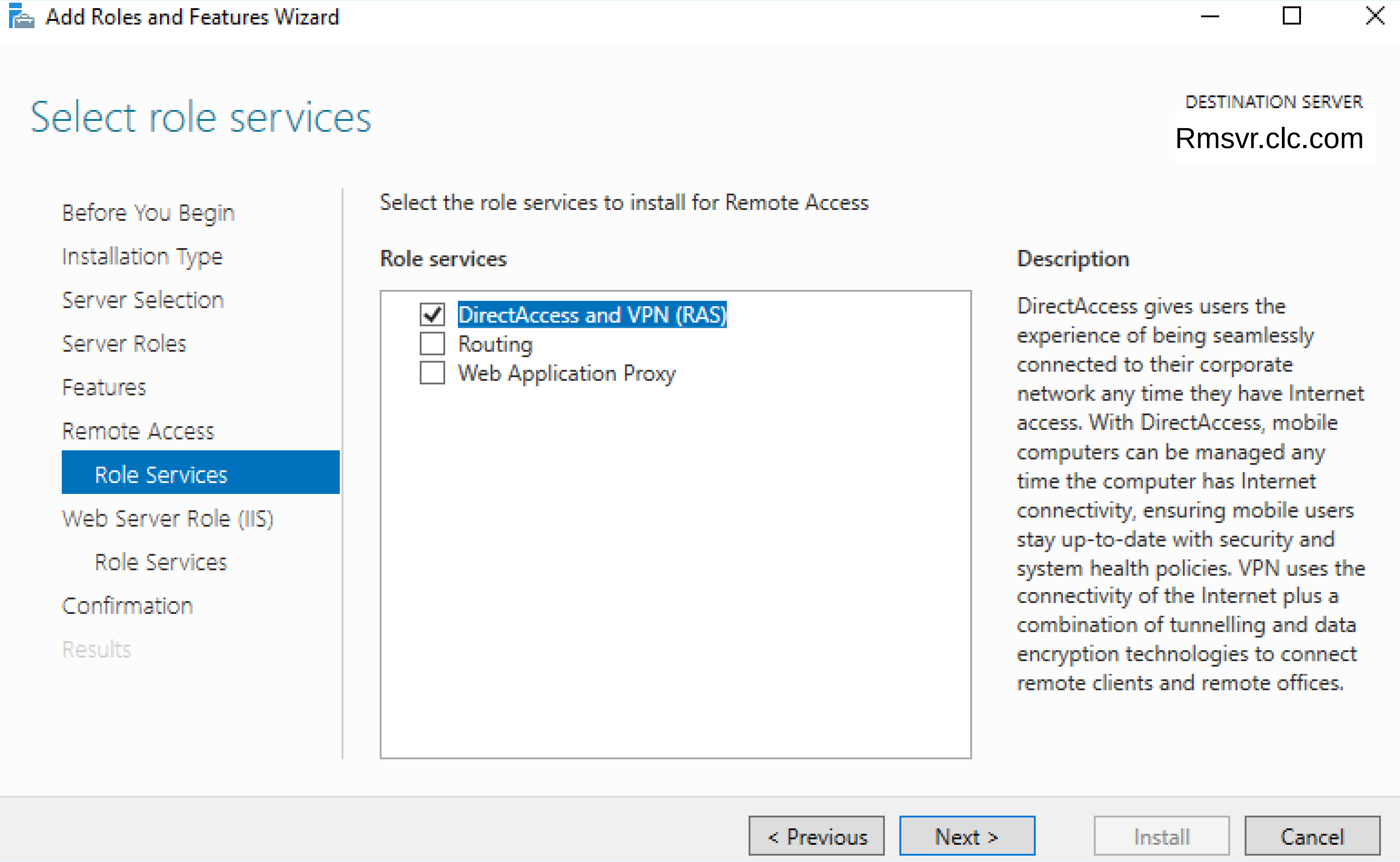
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- ☑ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

VPN

Install and Configure: Add Remote Access Role



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
Rmsvr.clc.com

Select the role services to install for Remote Access

Role services

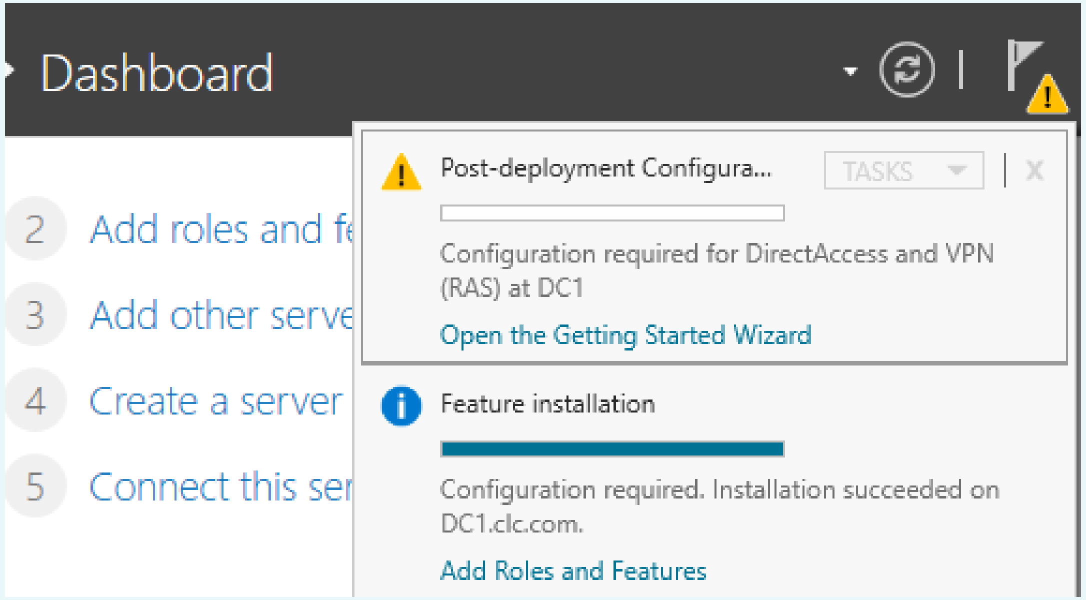
☑ DirectAccess and VPN (RAS)
□ Routing
□ Web Application Proxy

Description

DirectAccess gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, mobile computers can be managed any time the computer has Internet connectivity, ensuring mobile users stay up-to-date with security and system health policies. VPN uses the connectivity of the Internet plus a combination of tunnelling and data encryption technologies to connect remote clients and remote offices.

VPN

Install and Configure: Configure VPN



Dashboard

2 Add roles and fe

3 Add other serve

4 Create a server

5 Connect this ser

Post-deployment Configura... TASKS

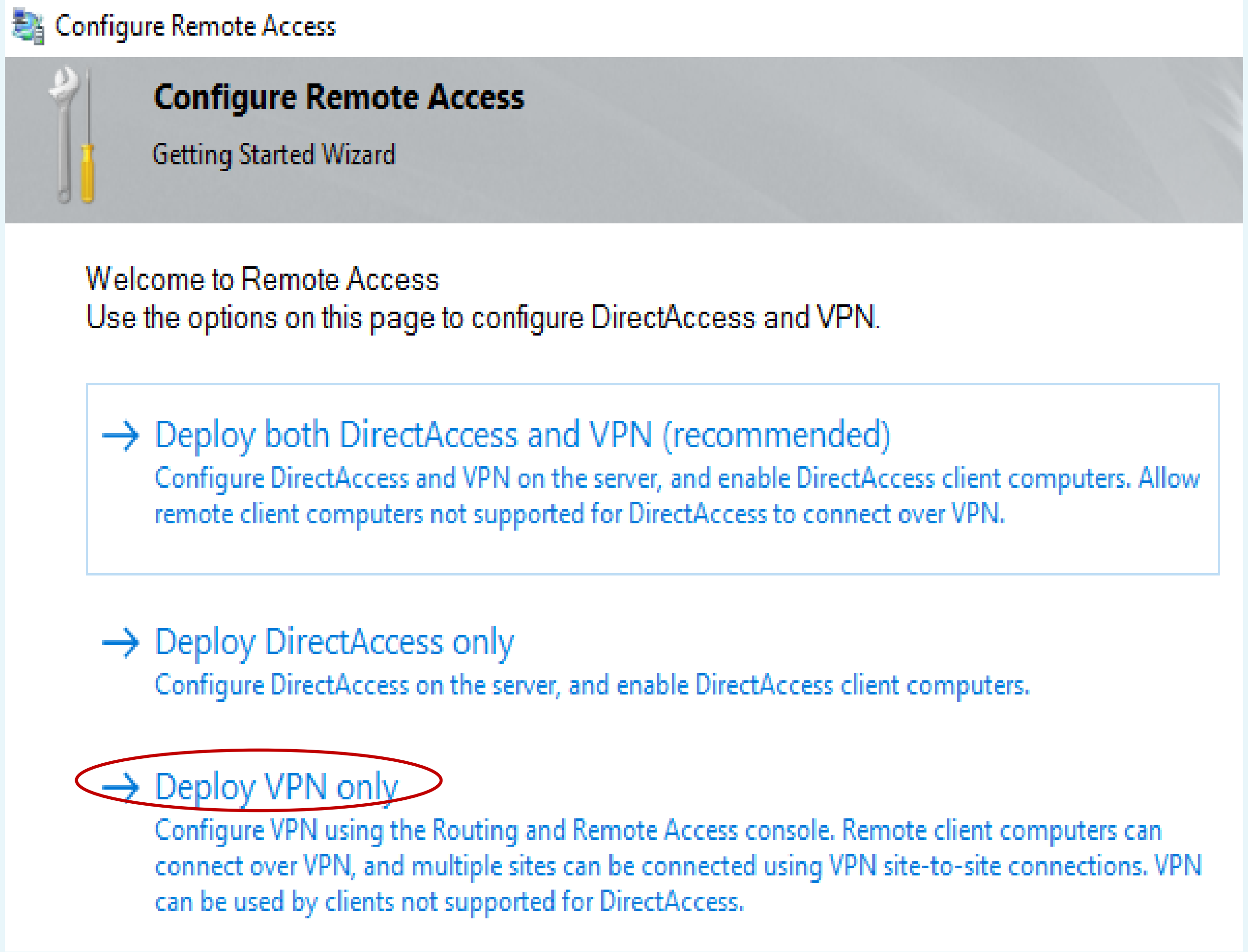
Configuration required for DirectAccess and VPN (RAS) at DC1

Open the Getting Started Wizard

Feature installation

Configuration required. Installation succeeded on DC1.clc.com.

Add Roles and Features



Configure Remote Access

Configure Remote Access

Getting Started Wizard

Welcome to Remote Access
Use the options on this page to configure DirectAccess and VPN.

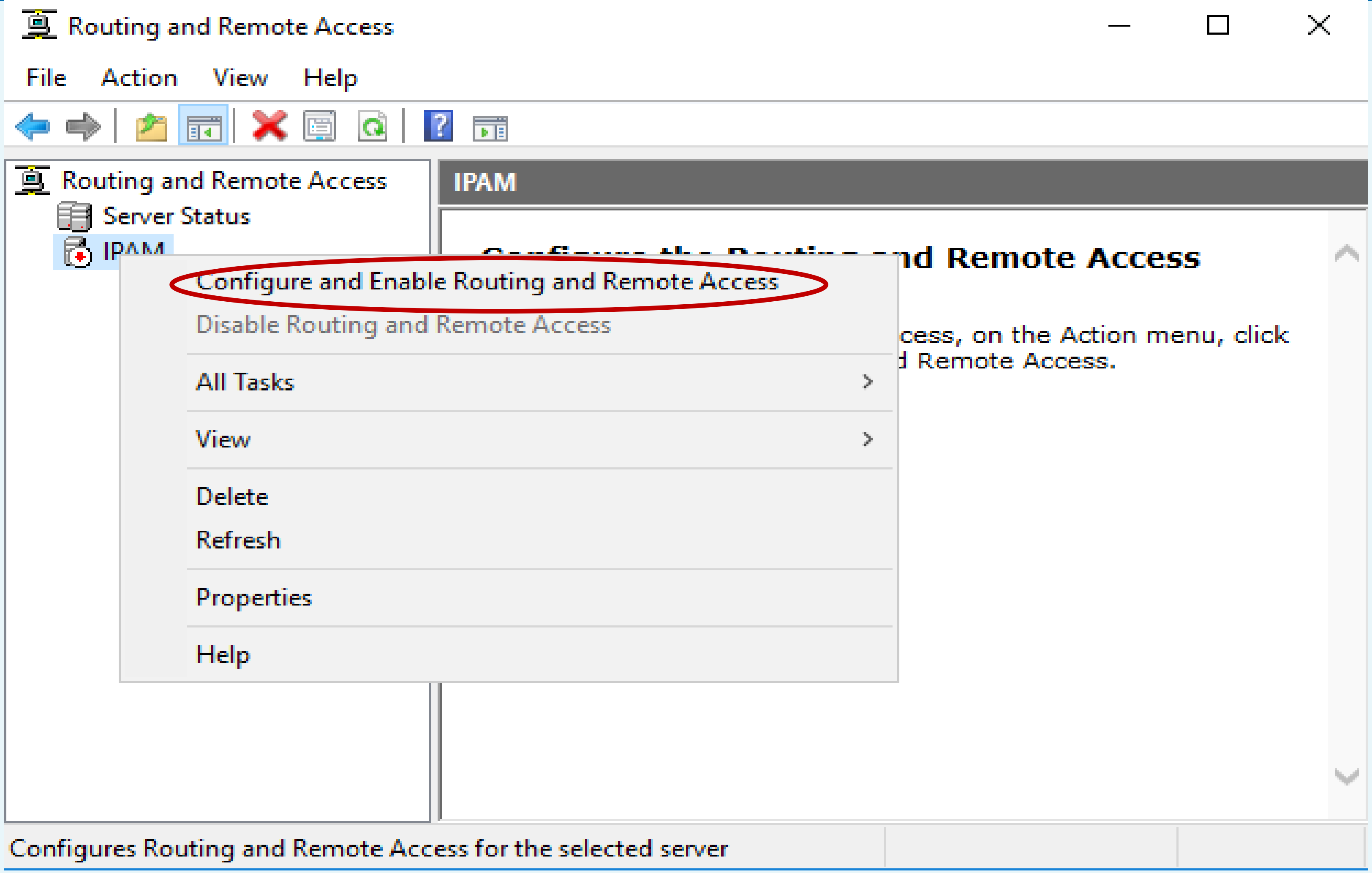
→ Deploy both DirectAccess and VPN (recommended)
Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.

→ Deploy DirectAccess only
Configure DirectAccess on the server, and enable DirectAccess client computers.

→ Deploy VPN only
Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.

VPN

Install and Configure: Configure VPN



Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
IPAM
IPAM
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help

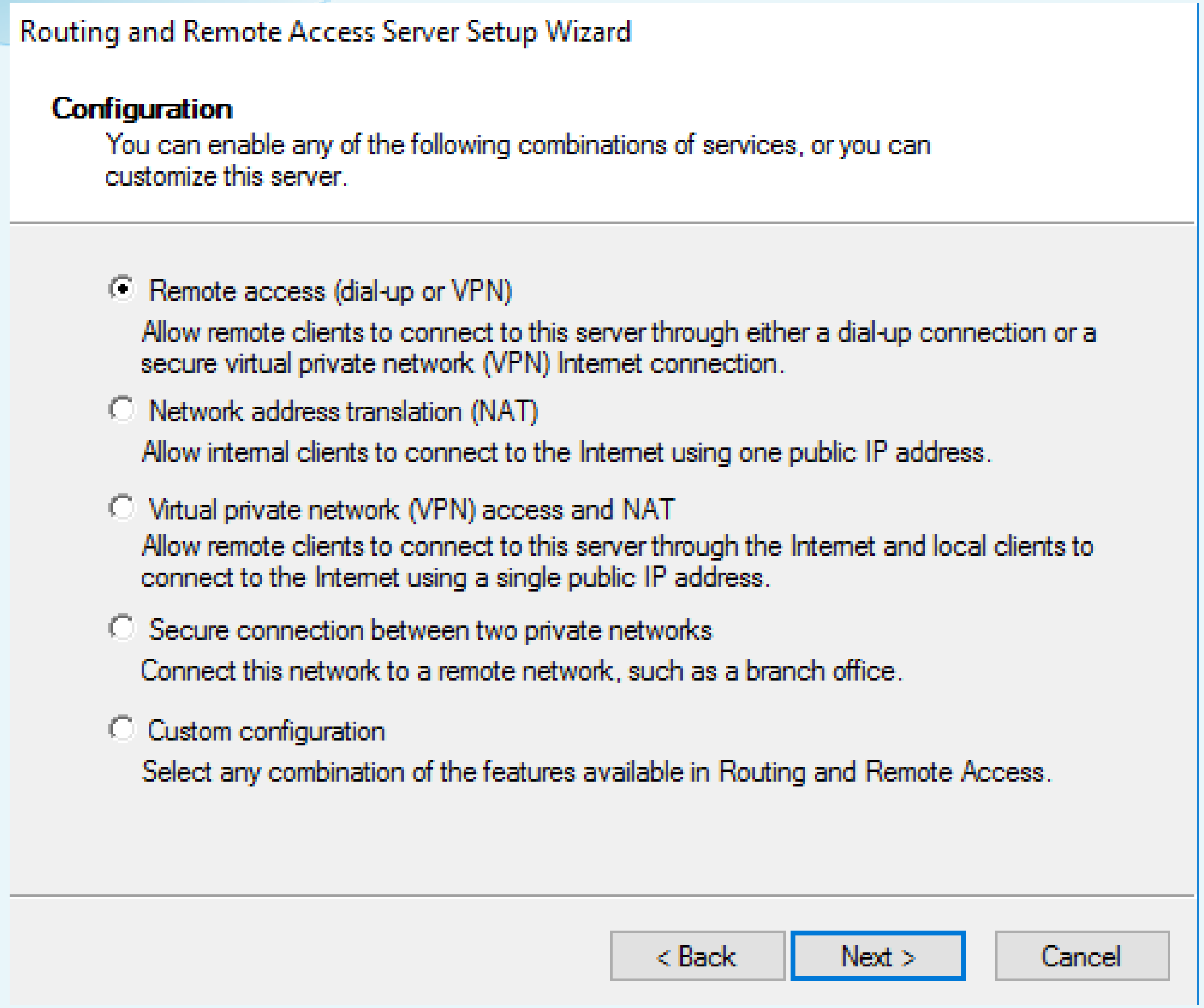
Configure the Routing and Remote Access

...cess, on the Action menu, click ...d Remote Access.

Configures Routing and Remote Access for the selected server

VPN

Install and Configure: Configure VPN



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

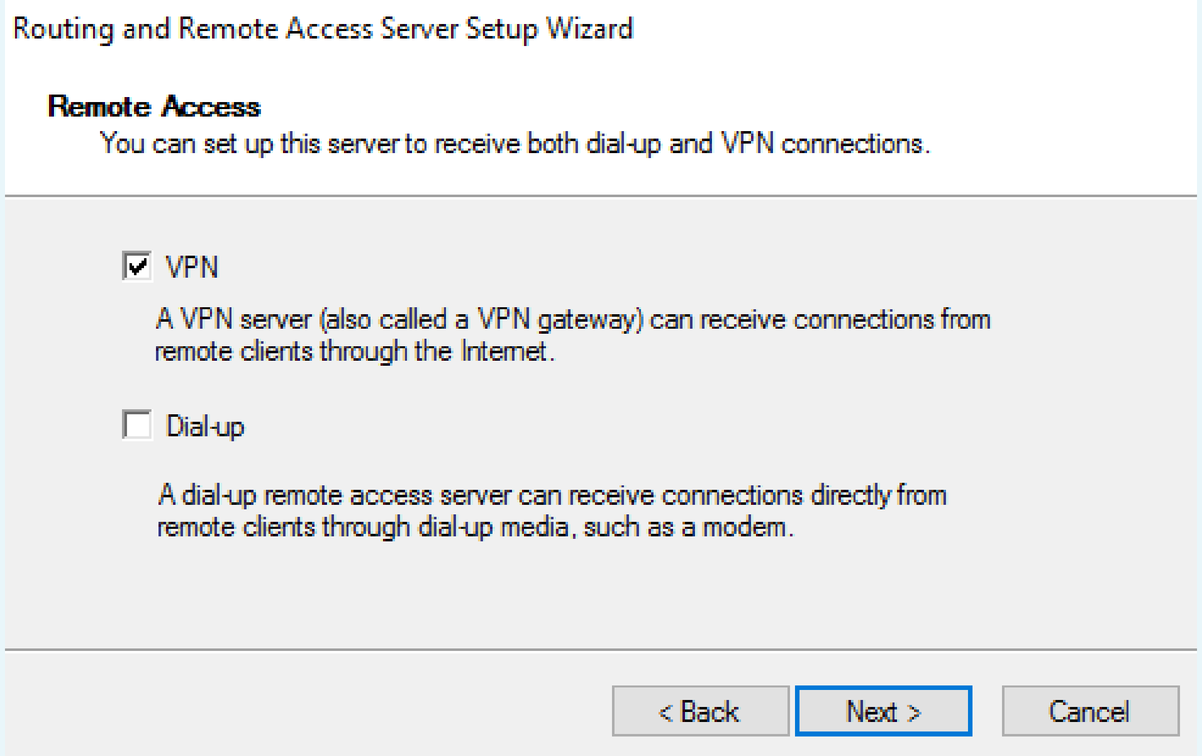
● Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.



Routing and Remote Access Server Setup Wizard

Remote Access

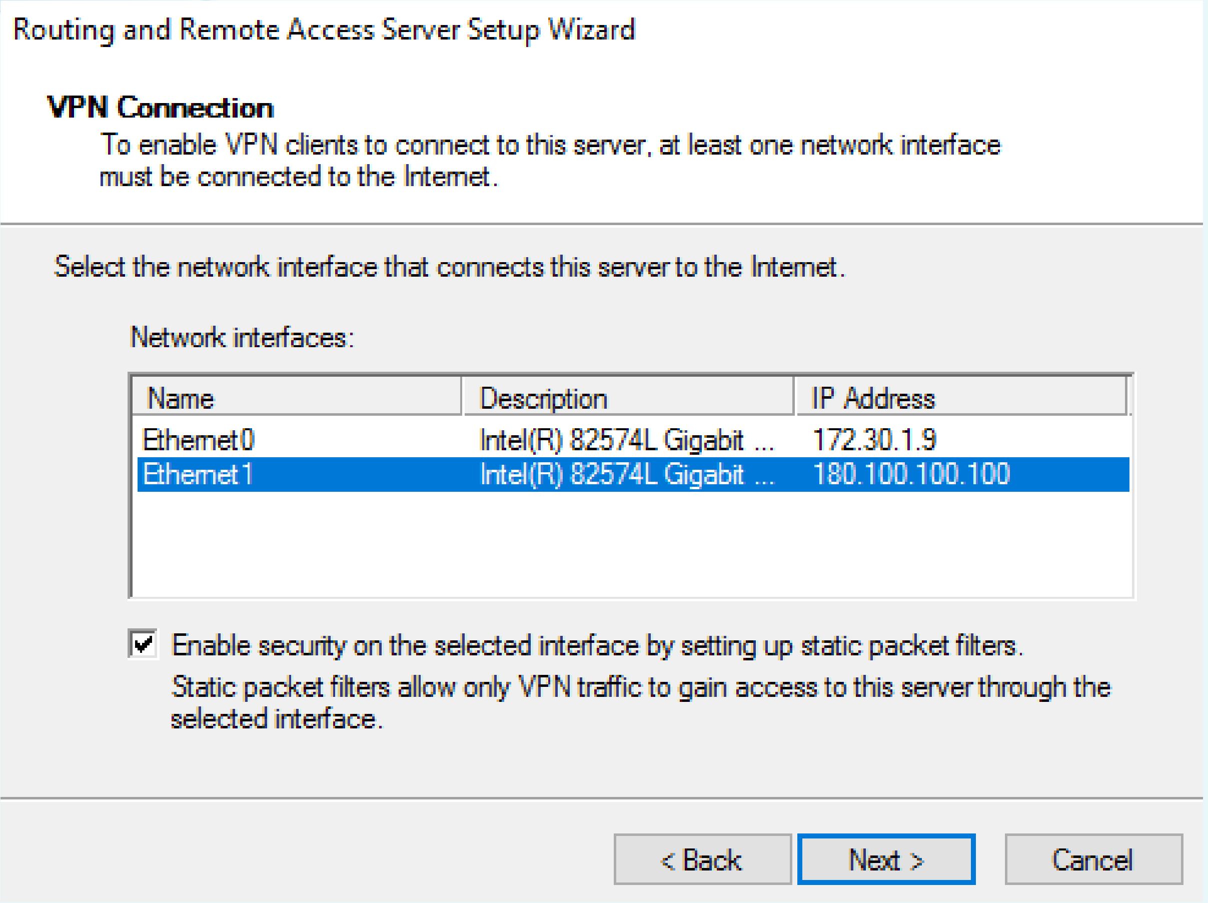
You can set up this server to receive both dial-up and VPN connections.

☑ VPN
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

□ Dial-up
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

VPN

Install and Configure: Configure VPN



Routing and Remote Access Server Setup Wizard

VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

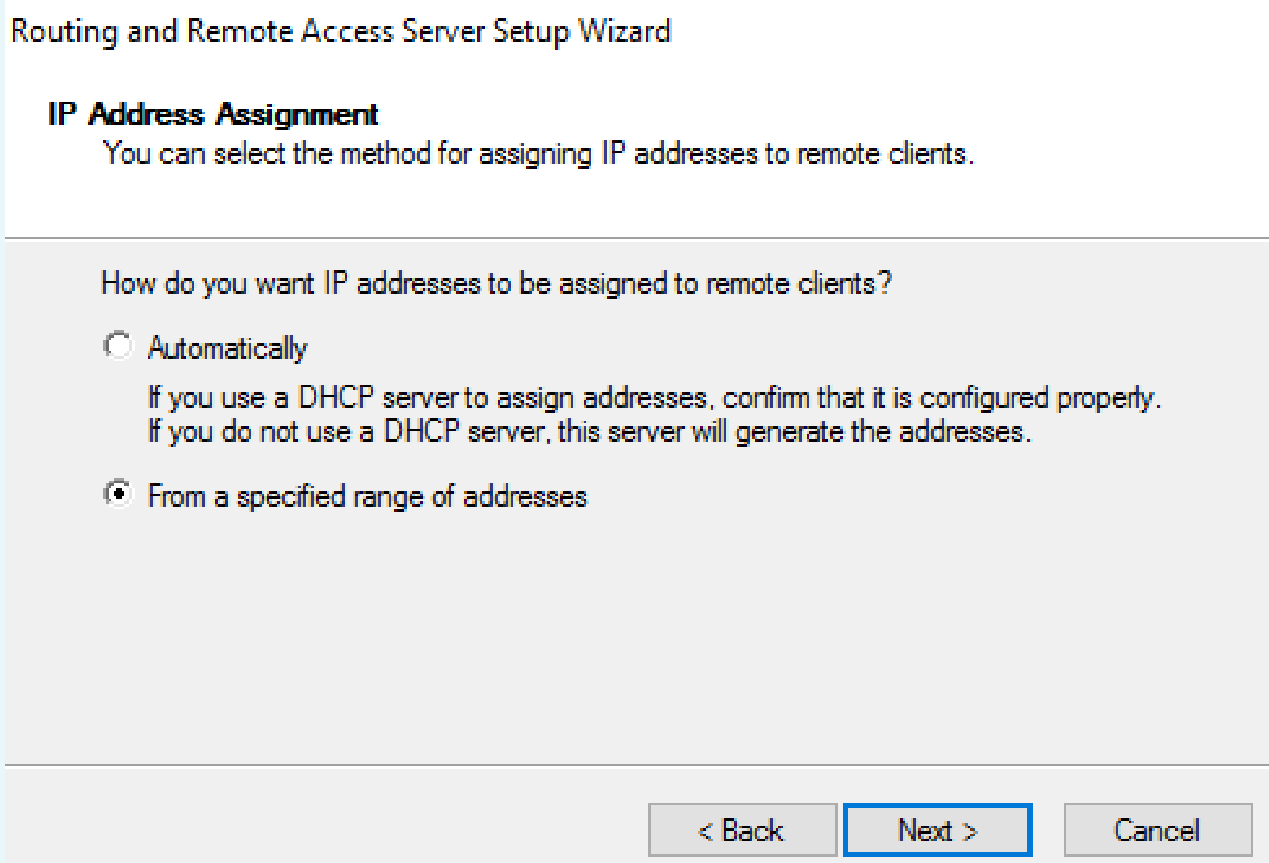
Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethernet0	Intel(R) 82574L Gigabit ...	172.30.1.9
Ethernet1	Intel(R) 82574L Gigabit ...	180.100.100.100

☑ Enable security on the selected interface by setting up static packet filters.

Static packet filters allow only VPN traffic to gain access to this server through the selected interface.



Routing and Remote Access Server Setup Wizard

IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

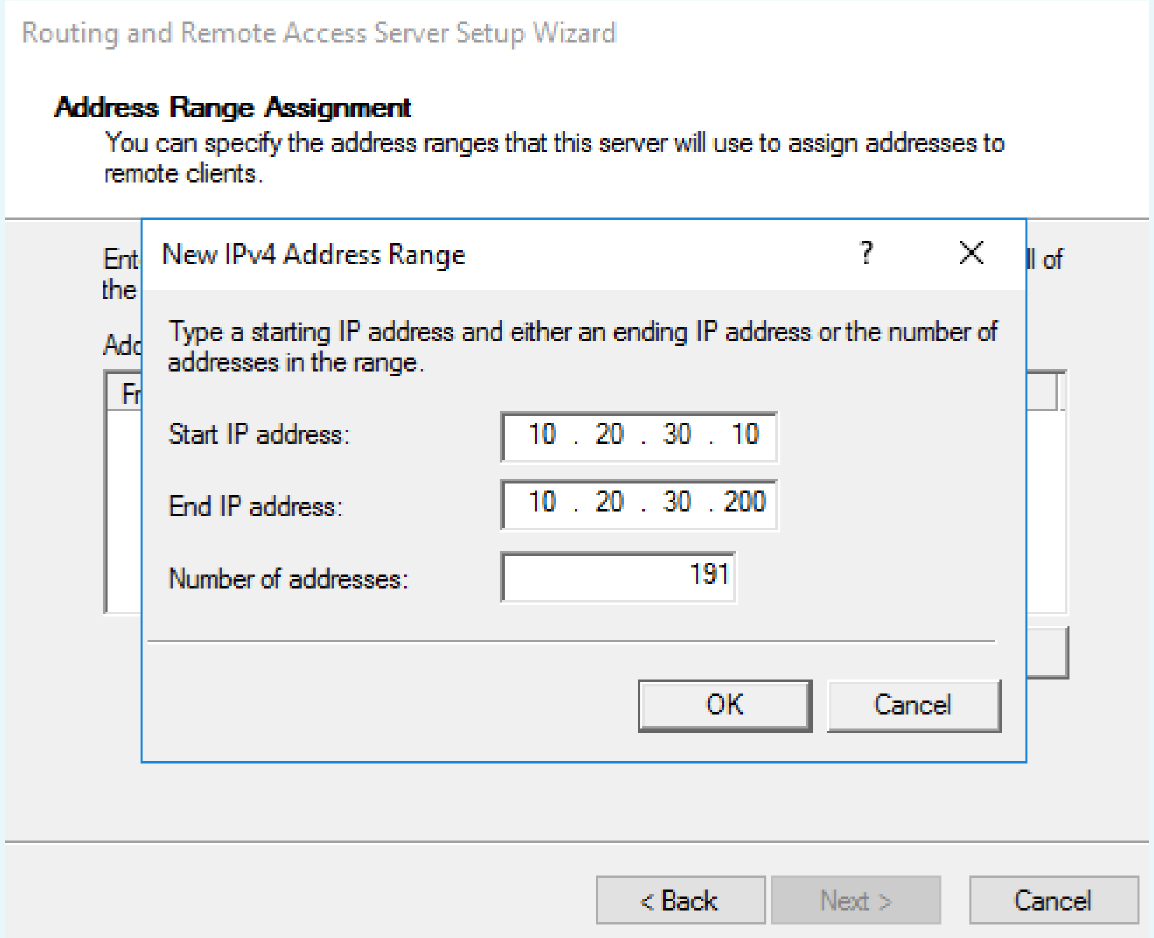
○ Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly. If you do not use a DHCP server, this server will generate the addresses.

● From a specified range of addresses

VPN

Install and Configure: Configure VPN



Routing and Remote Access Server Setup Wizard

Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

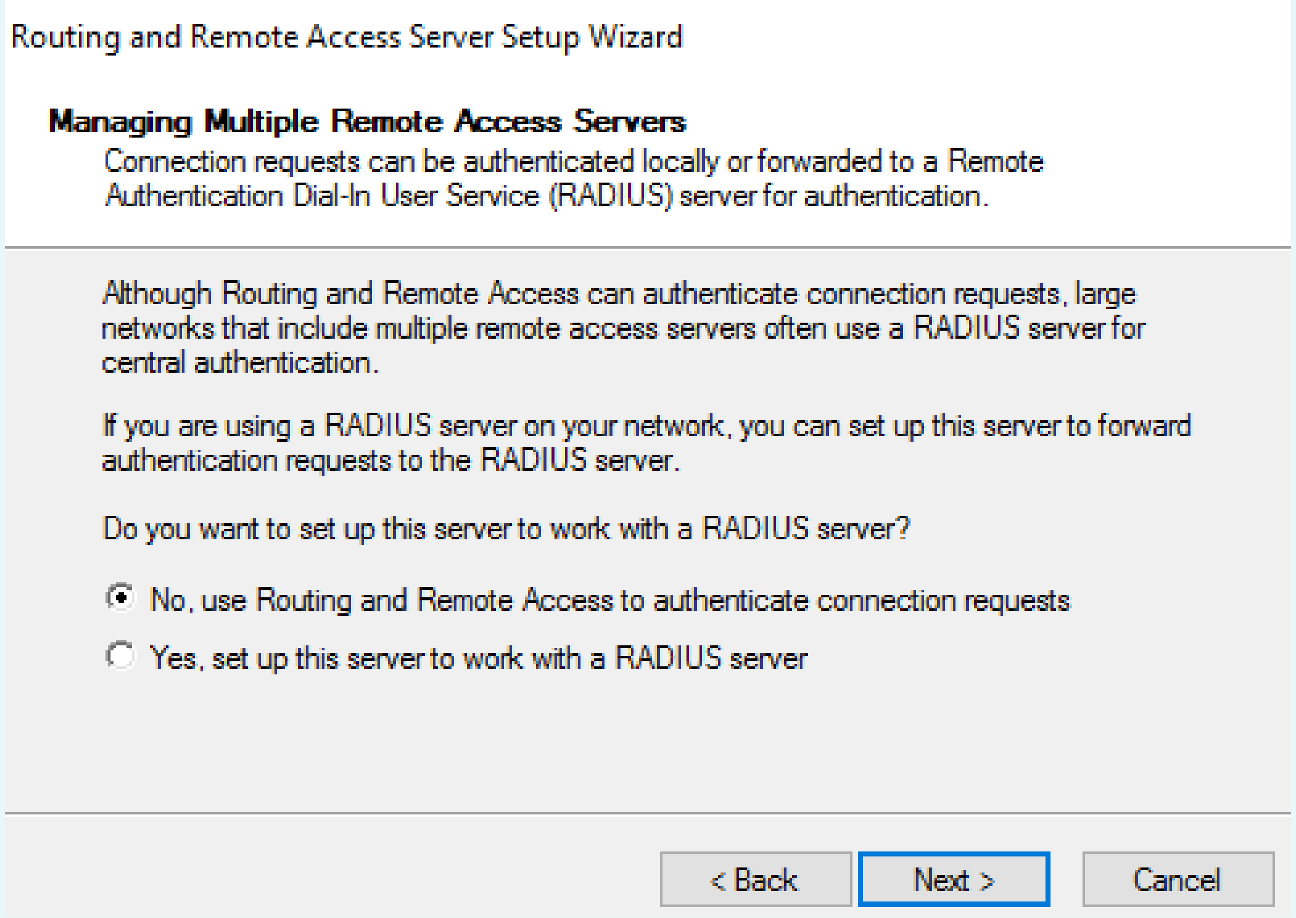
New IPv4 Address Range

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 10 . 20 . 30 . 10

End IP address: 10 . 20 . 30 . 200

Number of addresses: 191



Routing and Remote Access Server Setup Wizard

Managing Multiple Remote Access Servers

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

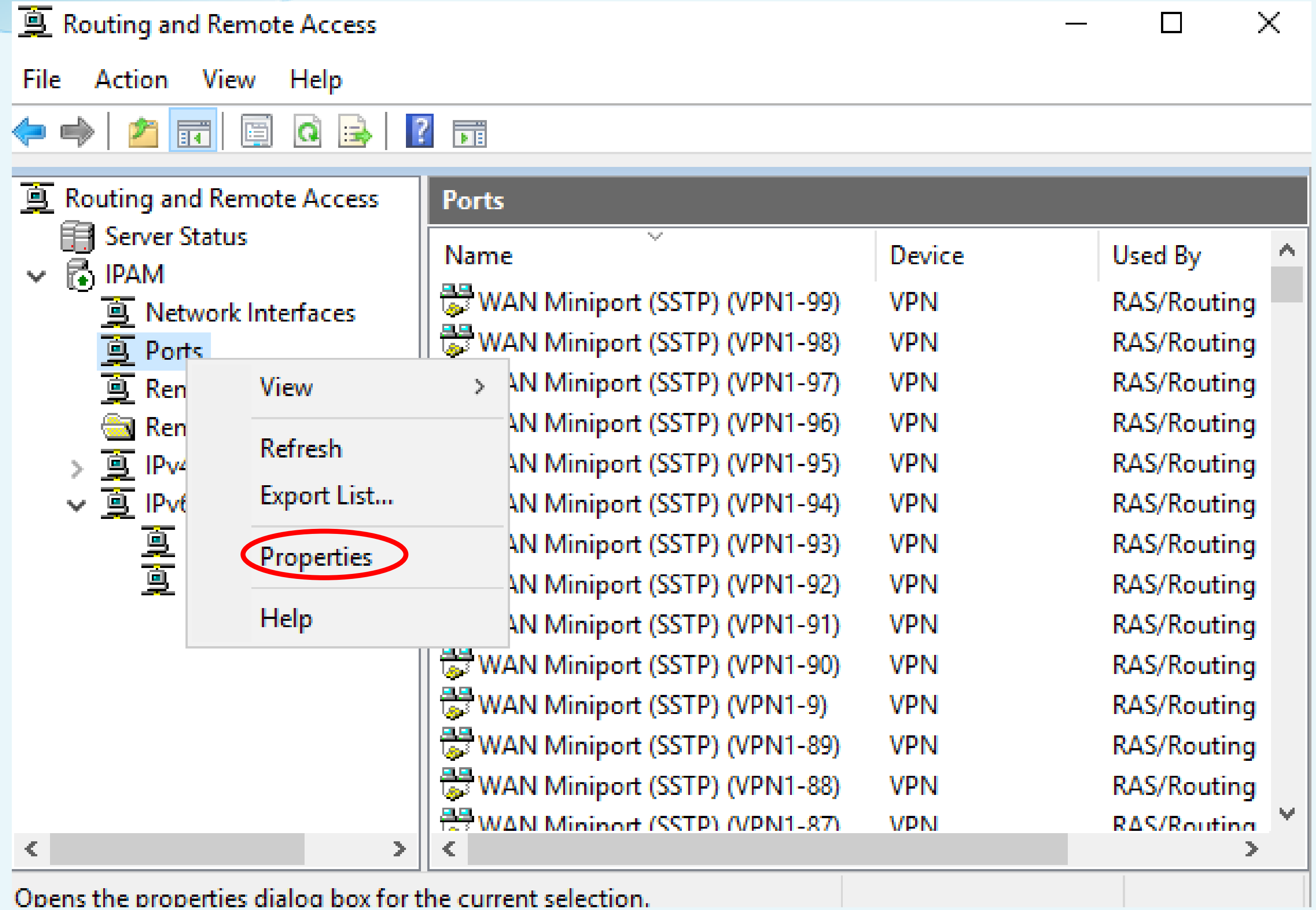
Do you want to set up this server to work with a RADIUS server?

● No, use Routing and Remote Access to authenticate connection requests

○ Yes, set up this server to work with a RADIUS server

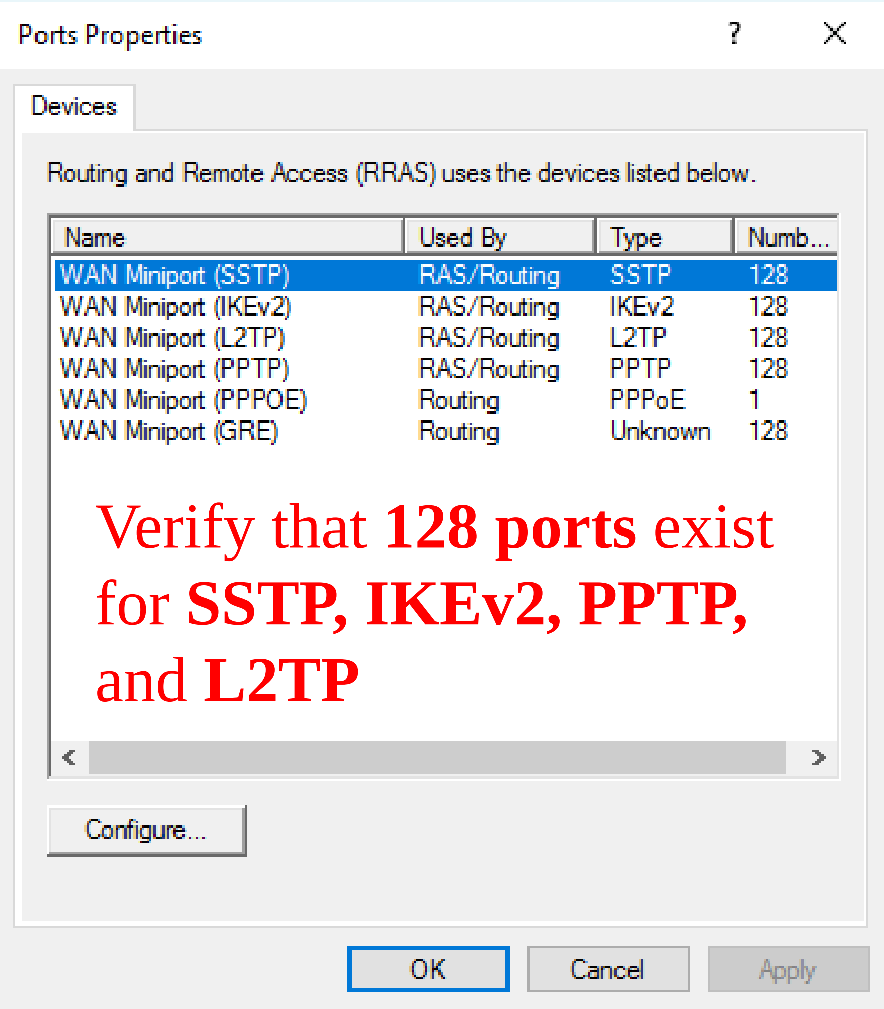
VPN

Install and Configure: Configure VPN



Name	Device	Used By
WAN Miniport (SSTP) (VPN1-99)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-98)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-97)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-96)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-95)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-94)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-93)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-92)	VPN	RAS/Routing
AN Miniport (SSTP) (VPN1-91)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-90)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-9)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-89)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-88)	VPN	RAS/Routing
WAN Miniport (SSTP) (VPN1-87)	VPN	RAS/Routing

Opens the properties dialog box for the current selection.



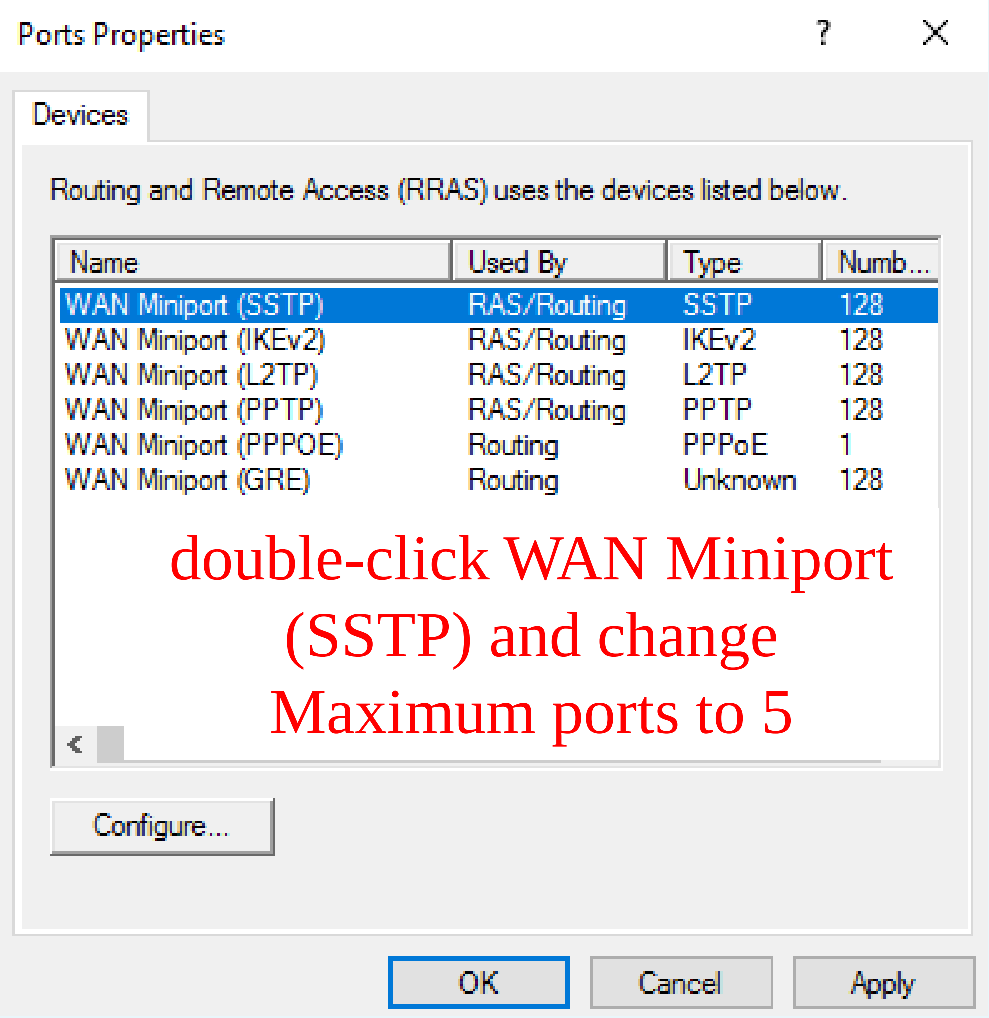
Routing and Remote Access (RRAS) uses the devices listed below.

Name	Used By	Type	Numb...
WAN Miniport (SSTP)	RAS/Routing	SSTP	128
WAN Miniport (IKEv2)	RAS/Routing	IKEv2	128
WAN Miniport (L2TP)	RAS/Routing	L2TP	128
WAN Miniport (PPTP)	RAS/Routing	PPTP	128
WAN Miniport (PPPOE)	Routing	PPPoE	1
WAN Miniport (GRE)	Routing	Unknown	128

Verify that **128 ports** exist for **SSTP, IKEv2, PPTP,** and **L2TP**

VPN

Install and Configure: Configure VPN



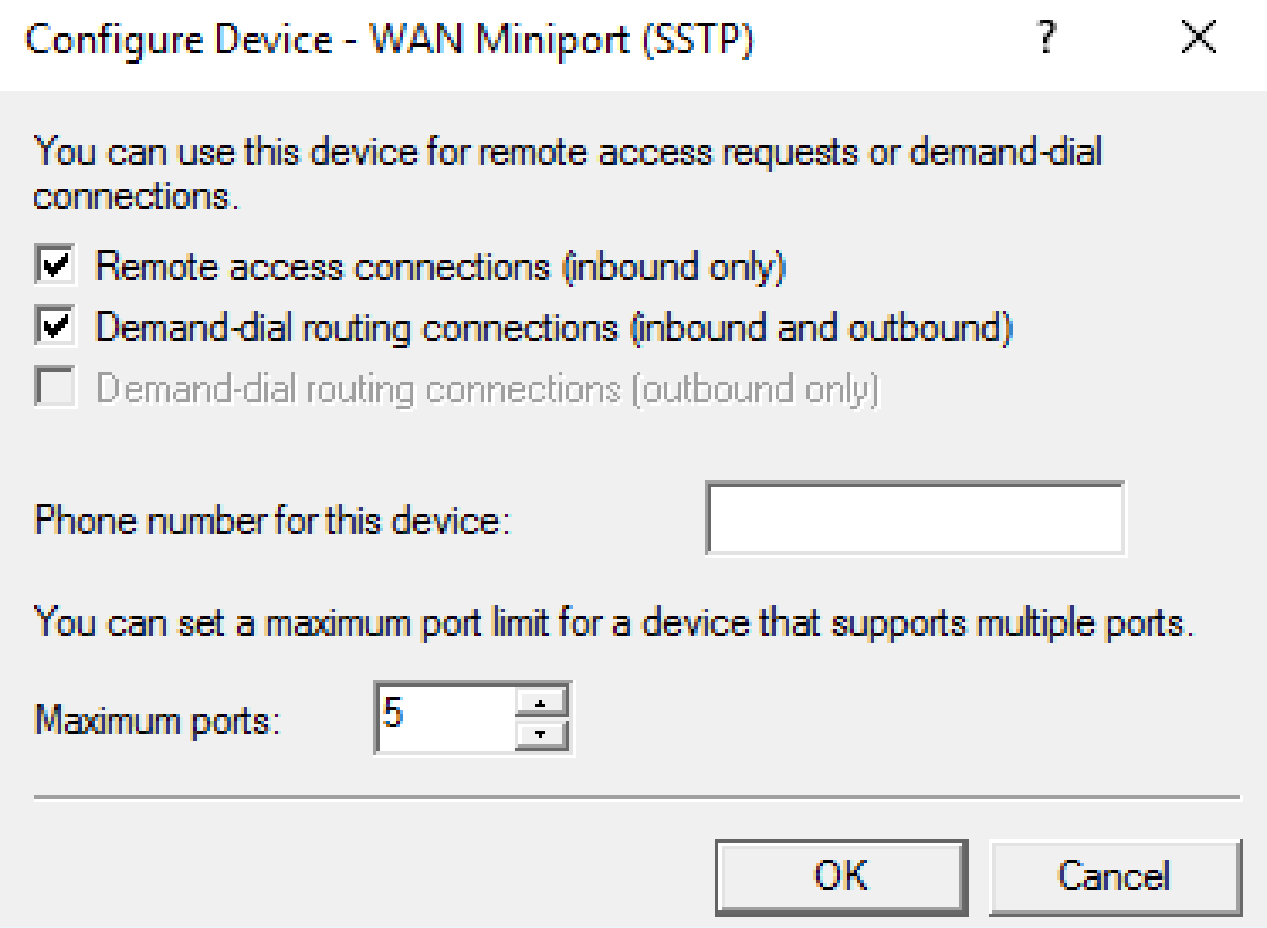
Ports Properties

Devices

Routing and Remote Access (RRAS) uses the devices listed below.

Name	Used By	Type	Numb...
WAN Miniport (SSTP)	RAS/Routing	SSTP	128
WAN Miniport (IKEv2)	RAS/Routing	IKEv2	128
WAN Miniport (L2TP)	RAS/Routing	L2TP	128
WAN Miniport (PPTP)	RAS/Routing	PPTP	128
WAN Miniport (PPPOE)	Routing	PPPoE	1
WAN Miniport (GRE)	Routing	Unknown	128

double-click WAN Miniport (SSTP) and change Maximum ports to 5



Configure Device - WAN Miniport (SSTP)

You can use this device for remote access requests or demand-dial connections.

☑ Remote access connections (inbound only)

☑ Demand-dial routing connections (inbound and outbound)

☐ Demand-dial routing connections (outbound only)

Phone number for this device:

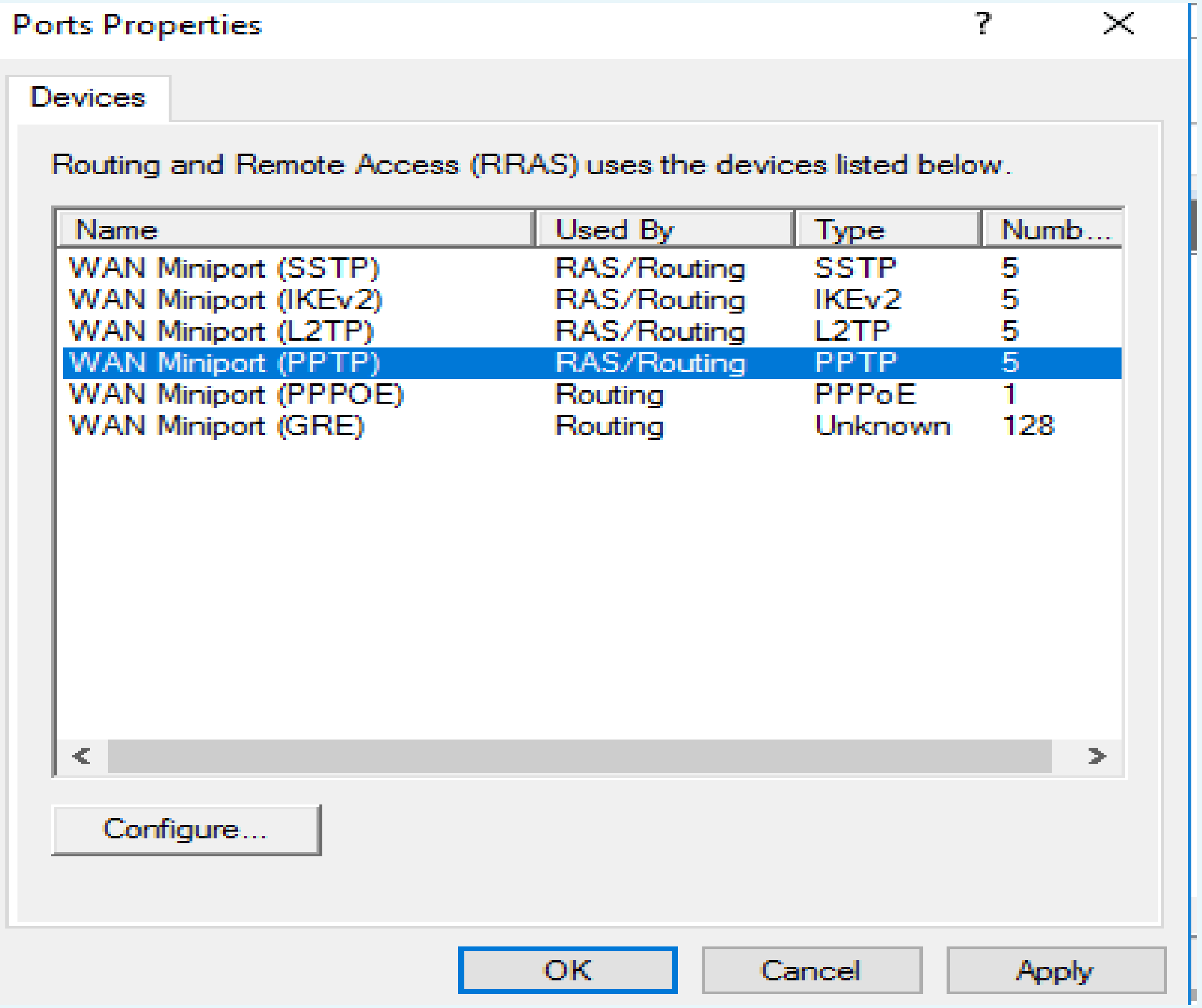
You can set a maximum port limit for a device that supports multiple ports.

Maximum ports: 5

VPN

Install and Configure: Configure VPN

Repeat to change Maximum ports to 5 for **IKEv2, PPTP,** and **L2TP**



Ports Properties

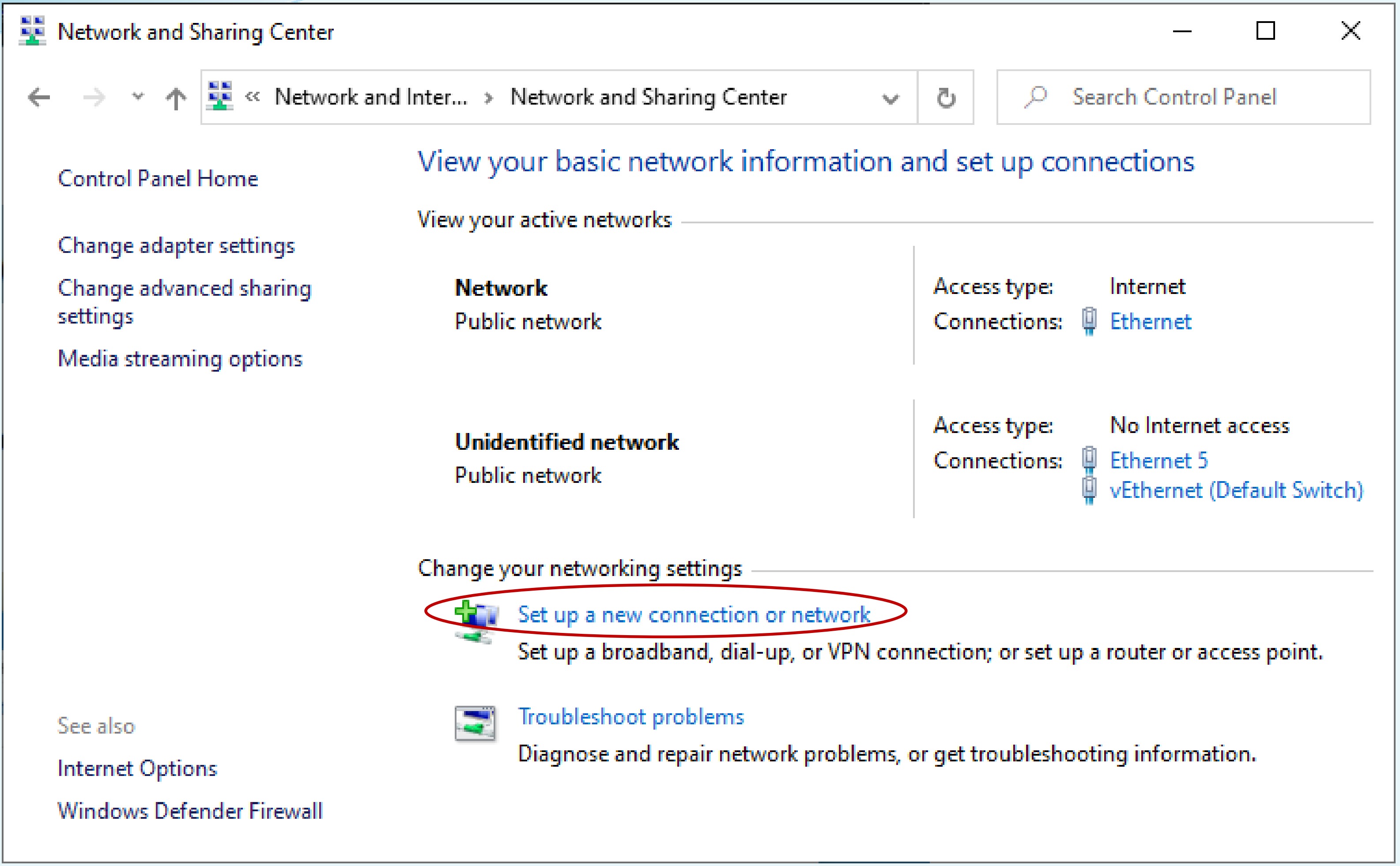
Devices

Routing and Remote Access (RRAS) uses the devices listed below.

Name	Used By	Type	Numb...
WAN Miniport (SSTP)	RAS/Routing	SSTP	5
WAN Miniport (IKEv2)	RAS/Routing	IKEv2	5
WAN Miniport (L2TP)	RAS/Routing	L2TP	5
WAN Miniport (PPTP)	RAS/Routing	PPTP	5
WAN Miniport (PPPOE)	Routing	PPPoE	1
WAN Miniport (GRE)	Routing	Unknown	128

VPN

Client Connectivity Testing



Network and Sharing Center

« Network and Inter... › Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

See also

Internet Options

Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Network
Public network

Access type: Internet
Connections: Ethernet

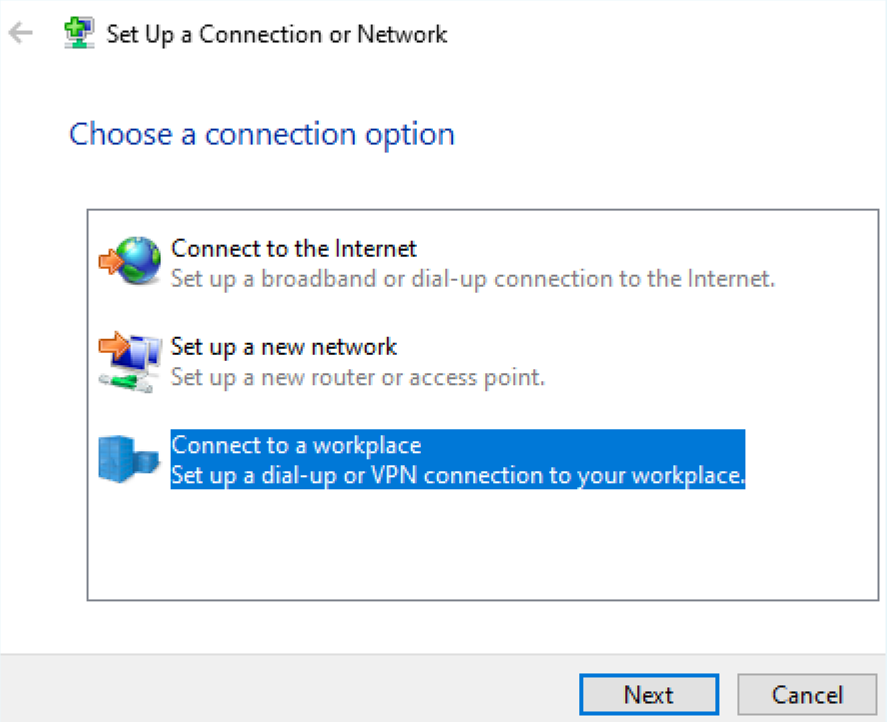
Unidentified network
Public network

Access type: No Internet access
Connections: Ethernet 5
vEthernet (Default Switch)

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

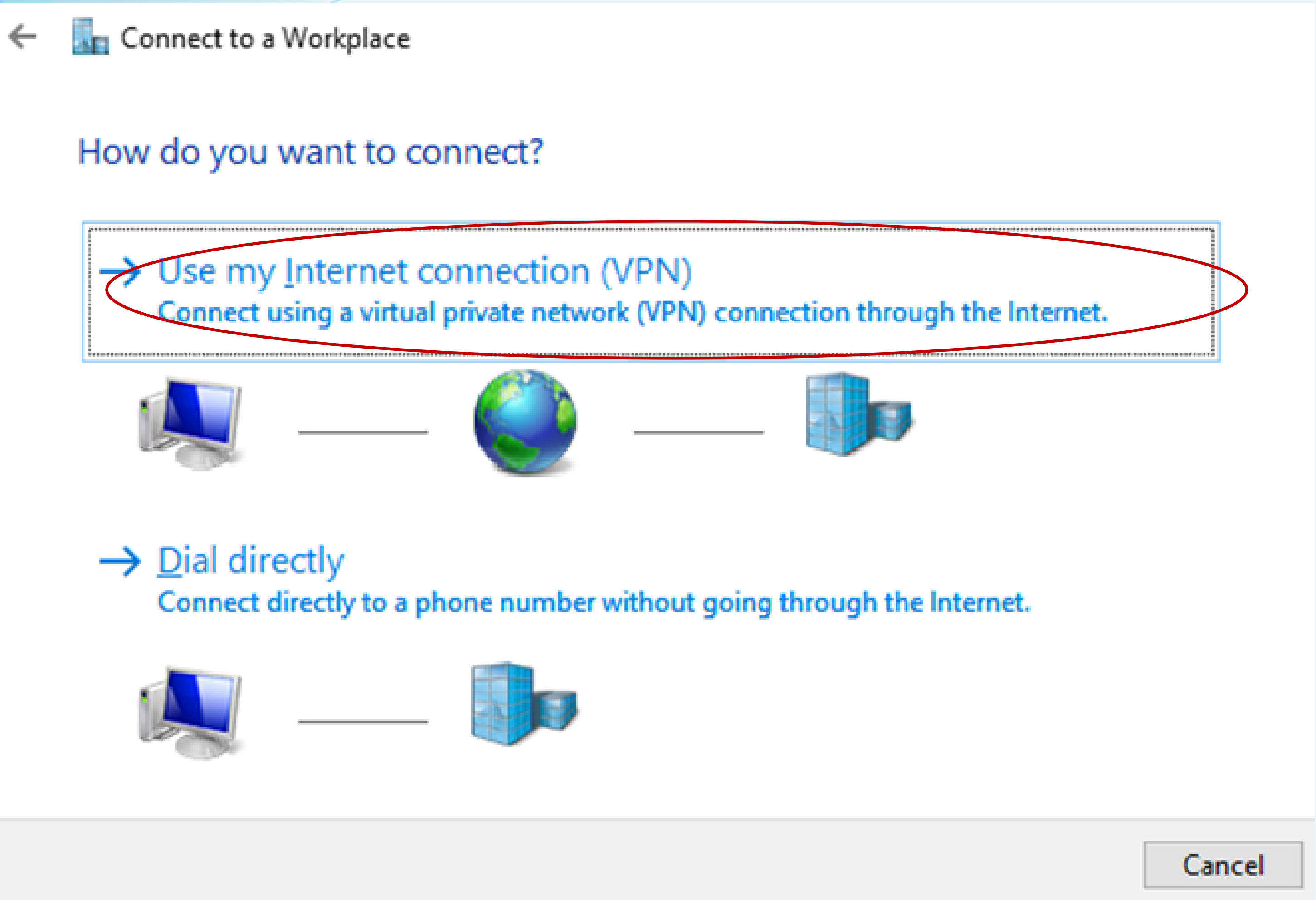
Set up a new network
Set up a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Next Cancel

VPN

Client Connectivity Testing

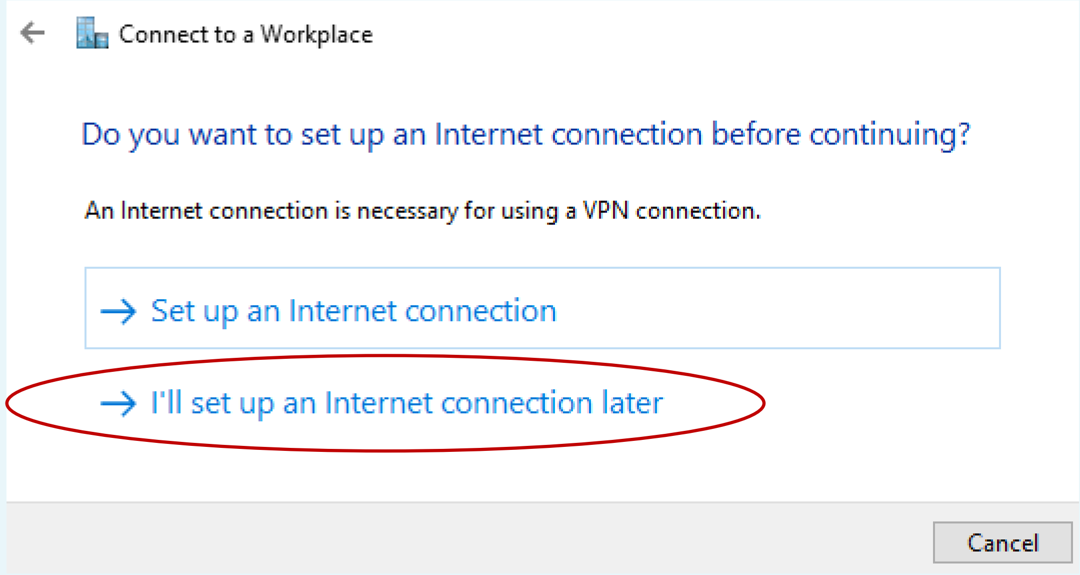


Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.



Connect to a Workplace

Do you want to set up an Internet connection before continuing?

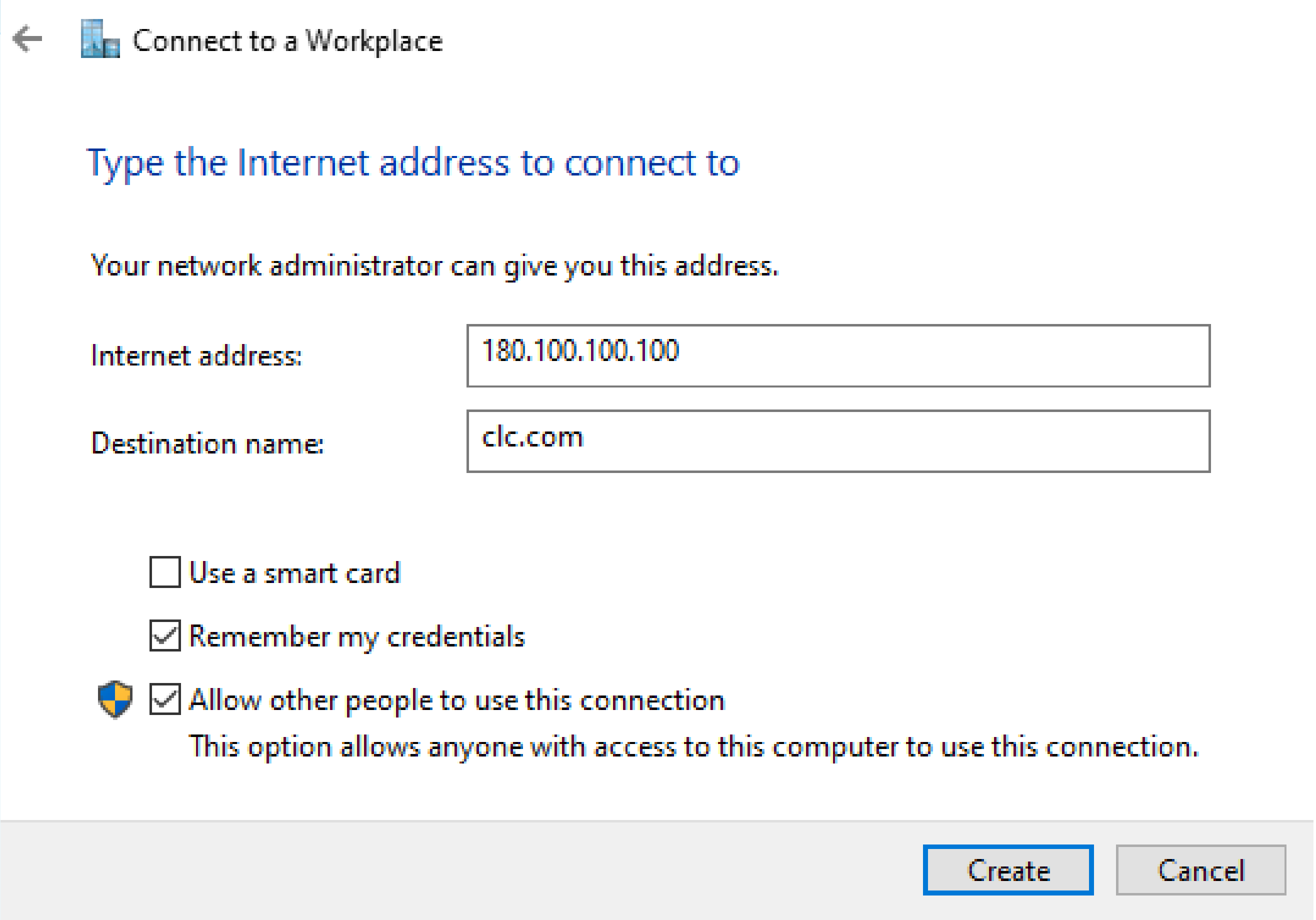
An Internet connection is necessary for using a VPN connection.

→ Set up an Internet connection

→ I'll set up an Internet connection later

VPN

Client Connectivity Testing



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

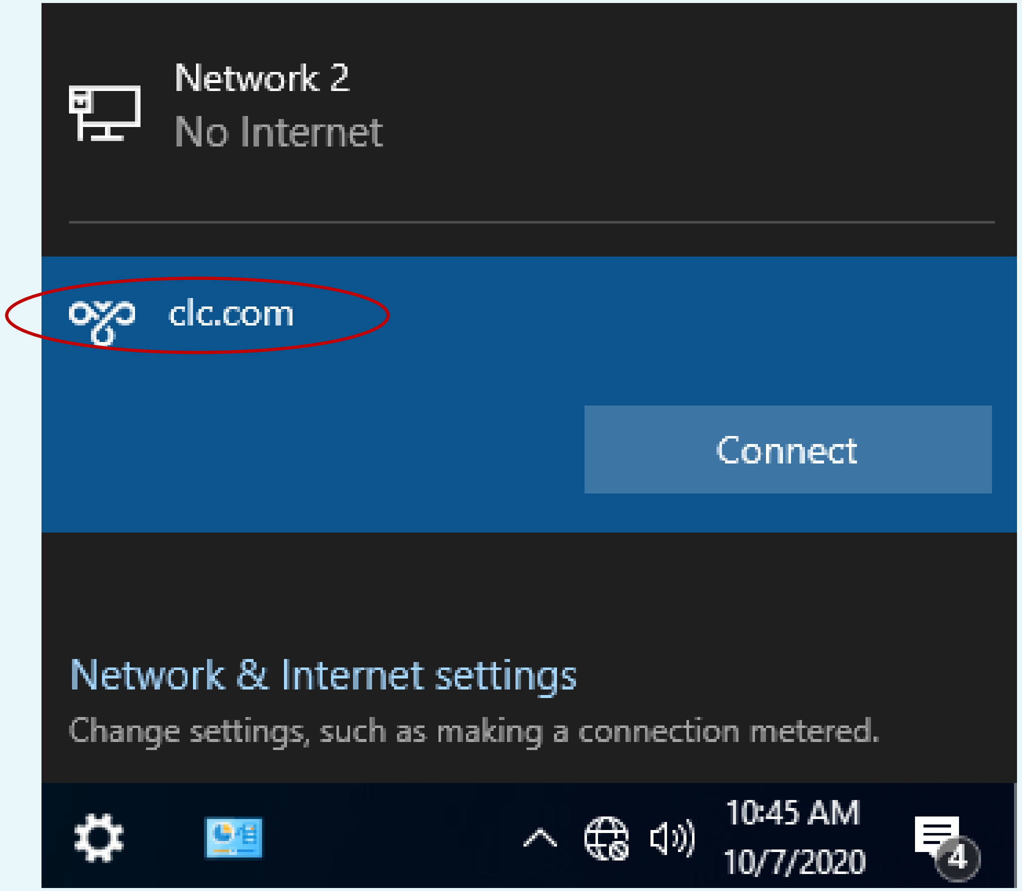
Internet address: 180.100.100.100

Destination name: clc.com

☐ Use a smart card

☑ Remember my credentials

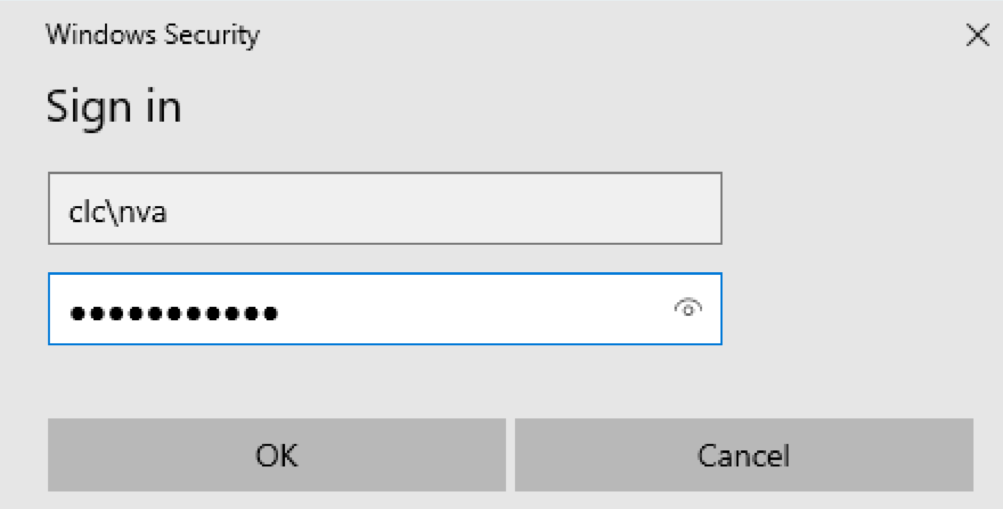
☑ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.



Network 2
No Internet
clc.com
Connect
Network & Internet settings
Change settings, such as making a connection metered.
10:45 AM
10/7/2020
4

VPN

Client Connectivity Testing

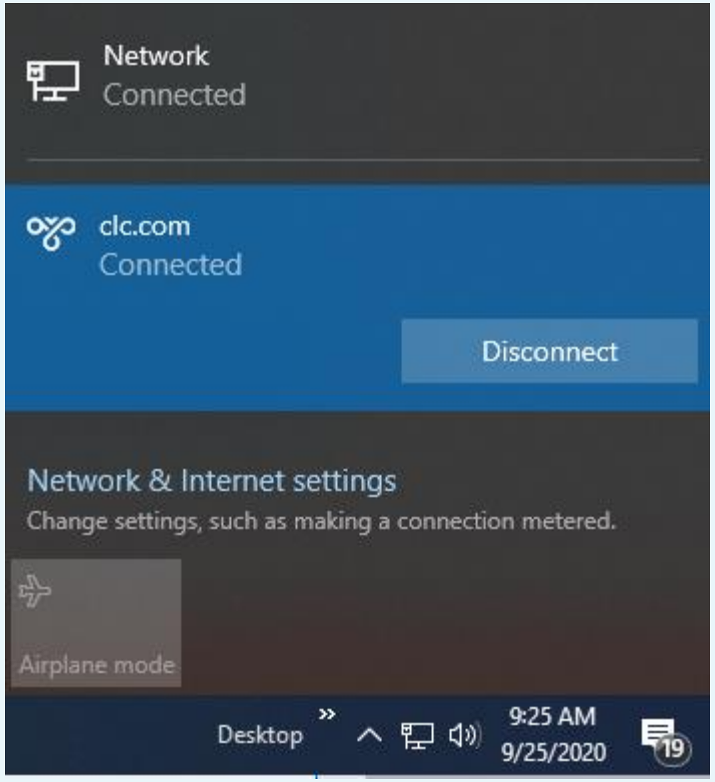


Windows Security

Sign in

clc\nva

●●●●●●●●●●●●



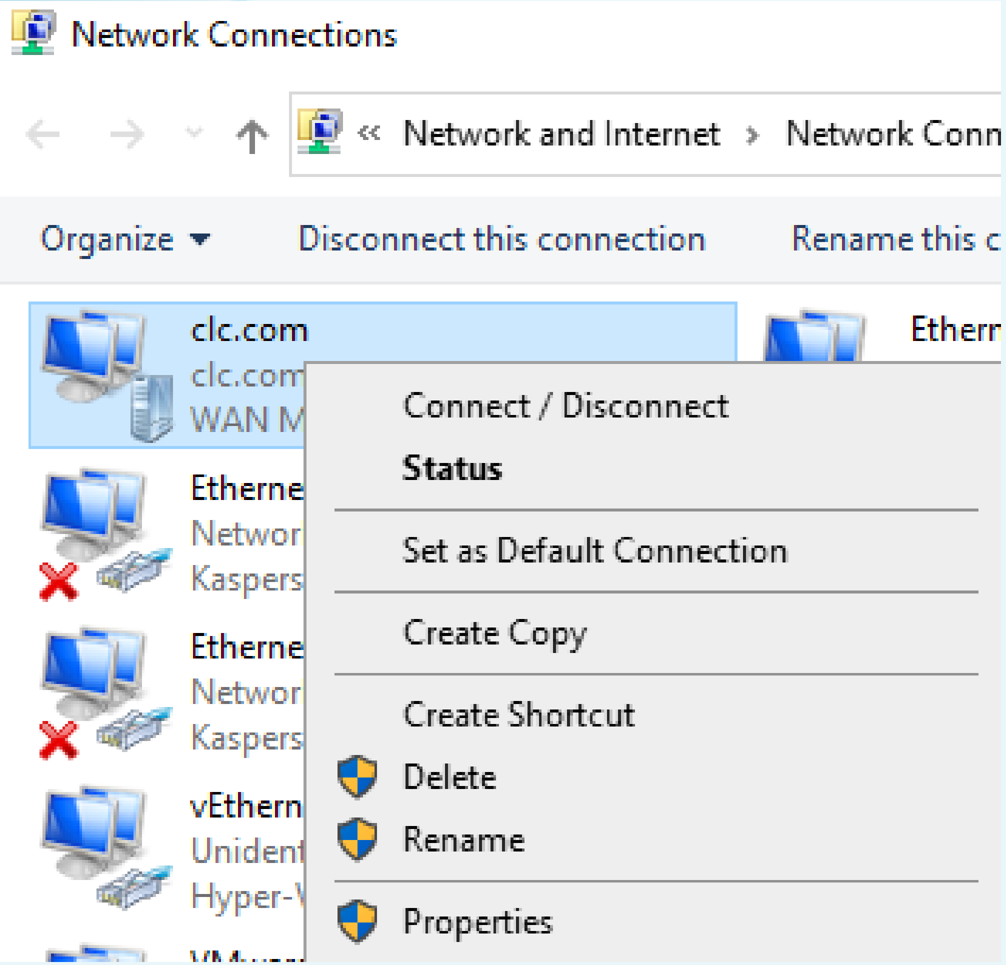
Network
Connected

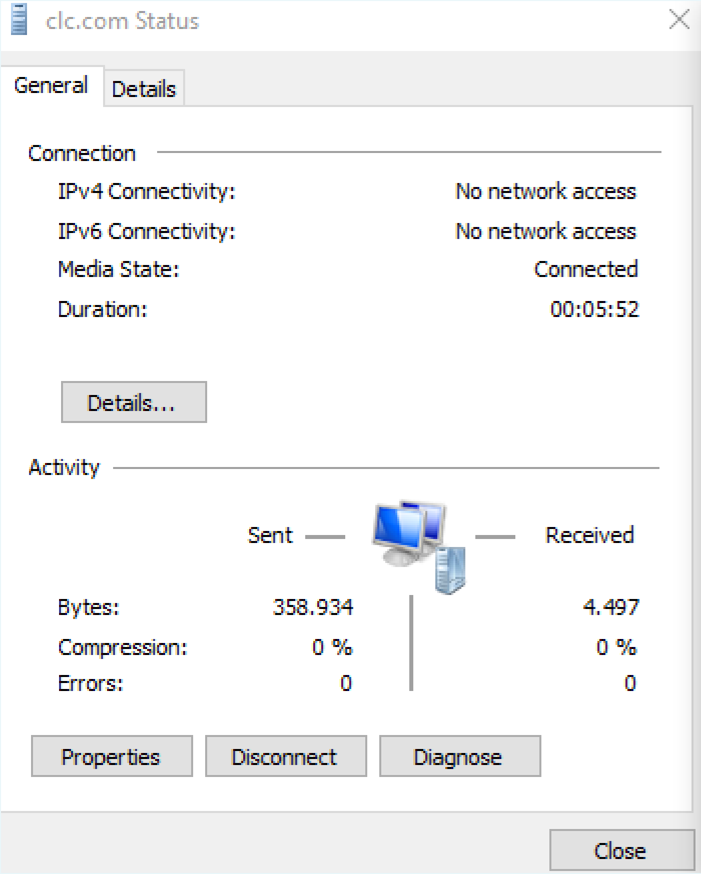
clc.com
Connected

Network & Internet settings
Change settings, such as making a connection metered.

VPN

Client Connectivity Testing




clc.com Status

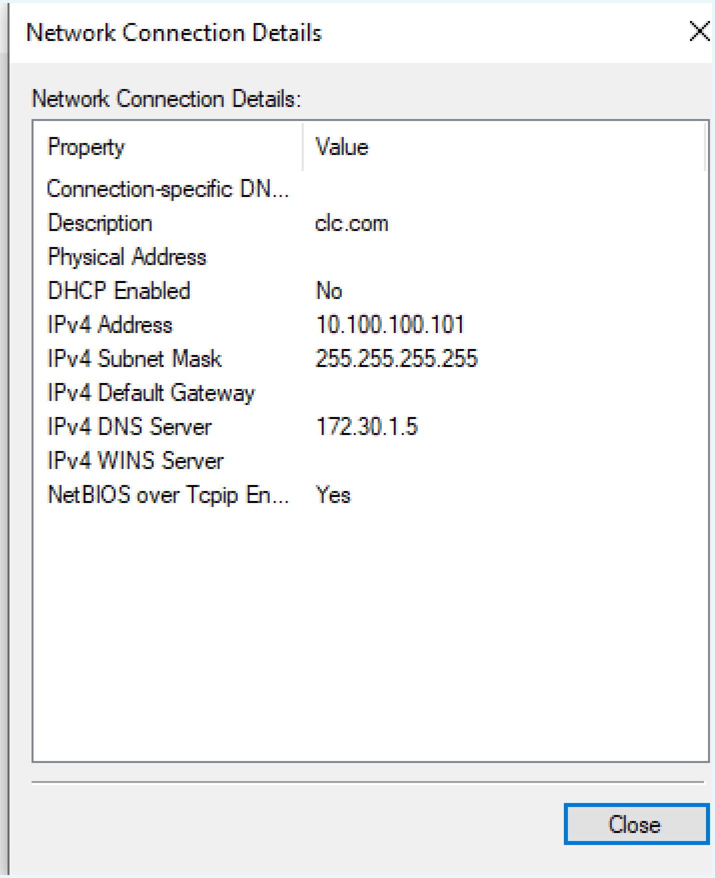
General | Details

Connection

IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Connected
Duration:	00:05:52

Activity

	Sent	Received
Bytes:	358.934	4.497
Compression:	0 %	0 %
Errors:	0	0

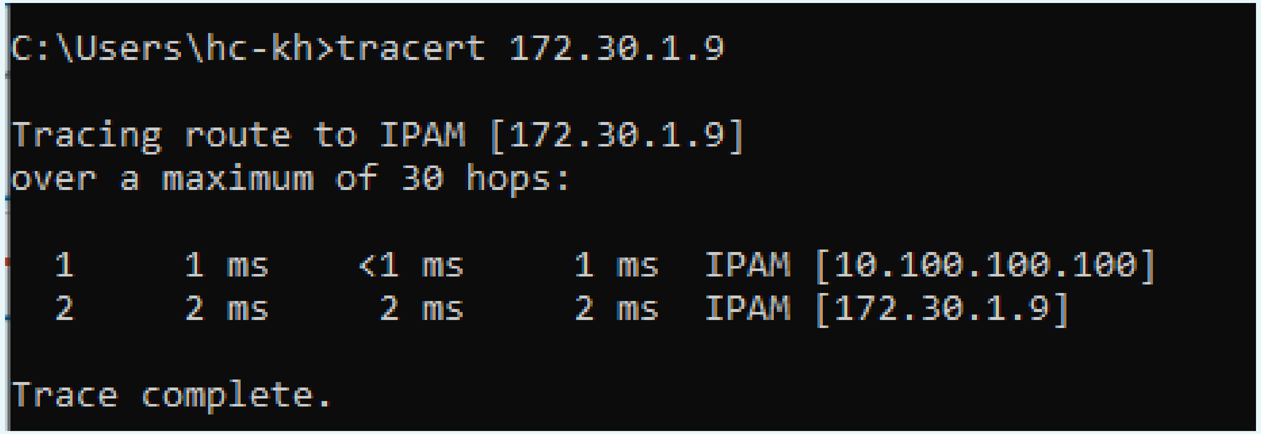

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	clc.com
Physical Address	
DHCP Enabled	No
IPv4 Address	10.100.100.101
IPv4 Subnet Mask	255.255.255.255
IPv4 Default Gateway	
IPv4 DNS Server	172.30.1.5
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

VPN

Client Connectivity Testing

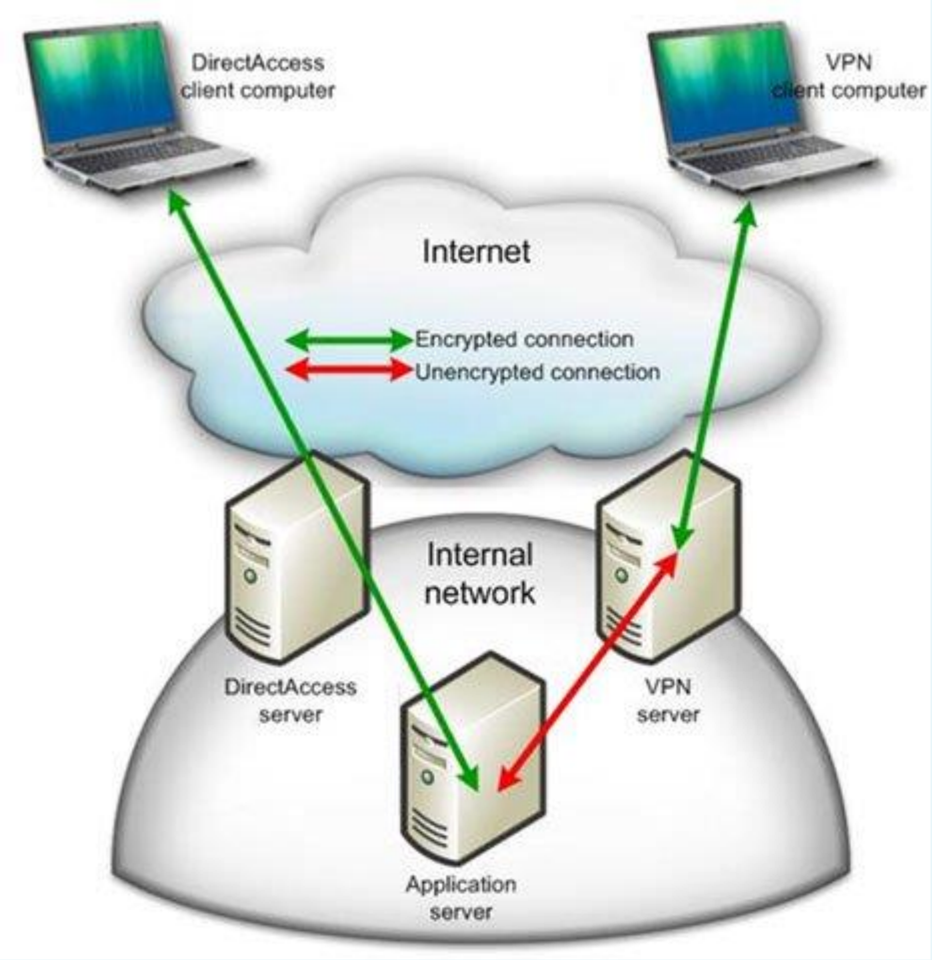


```
C:\Users\hc-kh>tracert 172.30.1.9

Tracing route to IPAM [172.30.1.9]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  IPAM [10.100.100.100]
  2     2 ms     2 ms     2 ms  IPAM [172.30.1.9]

Trace complete.
```

DirectAccess – automatic VPN

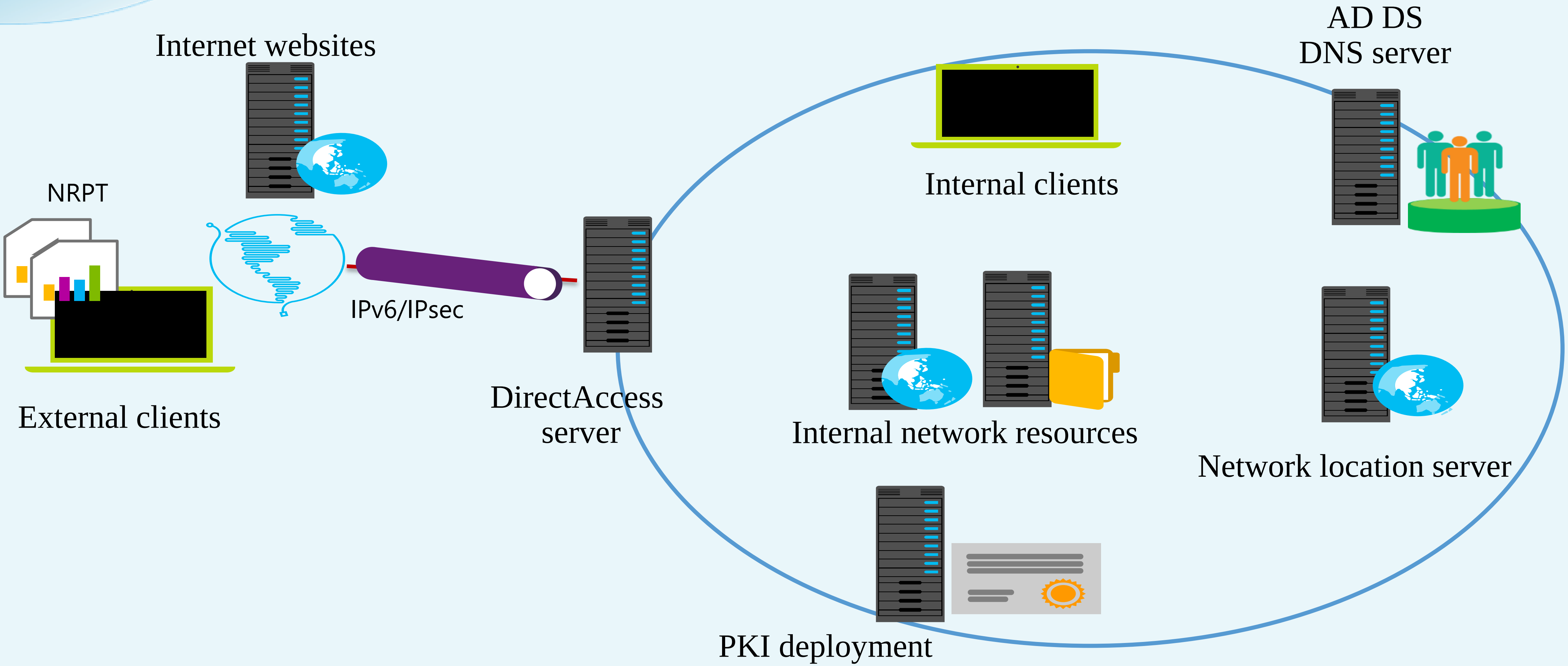
DirectAccess – automatic VPN

- Considered as an automatic VPN - the user don’t need to do anything to make DA connection
- As soon as the mobile computer receives an Internet connection, DA tunnels automatically built using available connection, without any user input
- Similar to VPN: securely connect remote computers to the corporate network
- Different from VPN: the method that employees use to make this connection possible.



DirectAccess

DA components



DirectAccess

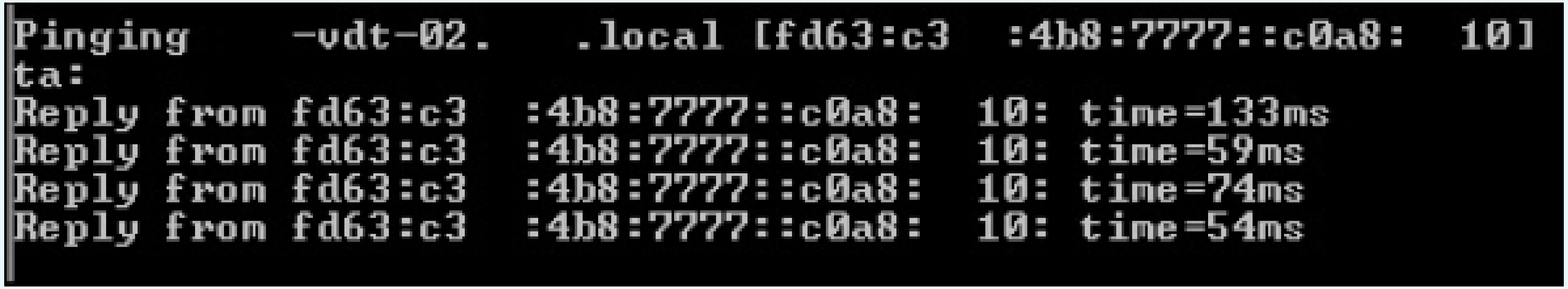
The truth about and IPv6

- The first version of DA requires the network utilize IPv6
- Fortunately, this requirement gone: you do not need IPv6 to use DA
- However, all of the traffic move over the Internet part of the connection (between the laptop and the DA) is IPv6 traffic
- The internal network is IPv4, and the DA server only has IPv4 addresses on it, but the DA tunnel is carrying the traffic using IPv6

DirectAccess

The truth about and IPv6

- As an example: you are sitting at home, working on the company laptop, DA connects you to the corporate network
- When open Command Prompt and ping one of servers from the laptop, this is what you see



```
Pinging    -vdt-02.   .local [fd63:c3  :4b8:7777::c0a8:  10]
ta:
Reply from fd63:c3  :4b8:7777::c0a8:  10: time=133ms
Reply from fd63:c3  :4b8:7777::c0a8:  10: time=59ms
Reply from fd63:c3  :4b8:7777::c0a8:  10: time=74ms
Reply from fd63:c3  :4b8:7777::c0a8:  10: time=54ms
```

DirectAccess

The truth about and IPv6

- DA laptop sends IPsec-encrypted IPv6 packets over the Internet to the DA server
- When receiving the packets, DA server has the capability to spin them down into IPv4 to send them to the destination server
- **For example**: when opening Outlook:
  - It tries to connect to Exchange server: packets flow over the DA tunnel as IPv6
  - Once these packets hit DA server: It figures out whether Exchange server is IPv4 or IPv6.
    - If the Exchange server is available via IPv6, the DA server will simply send the IPv6 packets along to the Exchange server
    - On the other hand, DA server will manipulate the IPv6 packet, changing it down into IPv4, and then send it on its way to the Exchange server.

DirectAccess

The truth about and IPv6

- The two technologies that handle this manipulation of the packets are **DNS64** and **NAT64**
- The purpose of these technologies is
  - to change the incoming IPv6 packet stream into IPv4 for the networks where it is required
  - and to spin the return traffic from IPv4 back up into IPv6 so that it can make its way back to the DA client computer over the IPv6-based IPsec tunnel

DirectAccess

Prerequisites: Domain joined

- The first big requirement is that the systems involved with DA need to be domain joined
- The DA servers and all of the client computers that you want to be DA connected need to be joined to a domain
- Domain membership is required for authentication purposes, and also because the DA client settings applied via Group Policy

DirectAccess

Prerequisites: client operating systems

- Not all of the Windows client operating systems contain the components that are necessary to make a DA connection work
- The operating systems support DA:
  - Windows 10 Enterprise
  - Windows 10 Education
  - Windows 8.0 or 8.1 Enterprise
  - Windows 7 Enterprise
  - Windows 7 Ultimate

DirectAccess

Prerequisites: One or two NICs?

- Two methods for implementing DA: 1) Single NIC mode; and 2) Edge mode with two NICs
- Single NIC mode
  - The NIC connected directly into the internal network, so that it had access to all of the internal resources
  - To get traffic from the Internet to DA server, Network Address Translation (NAT) is used

DirectAccess

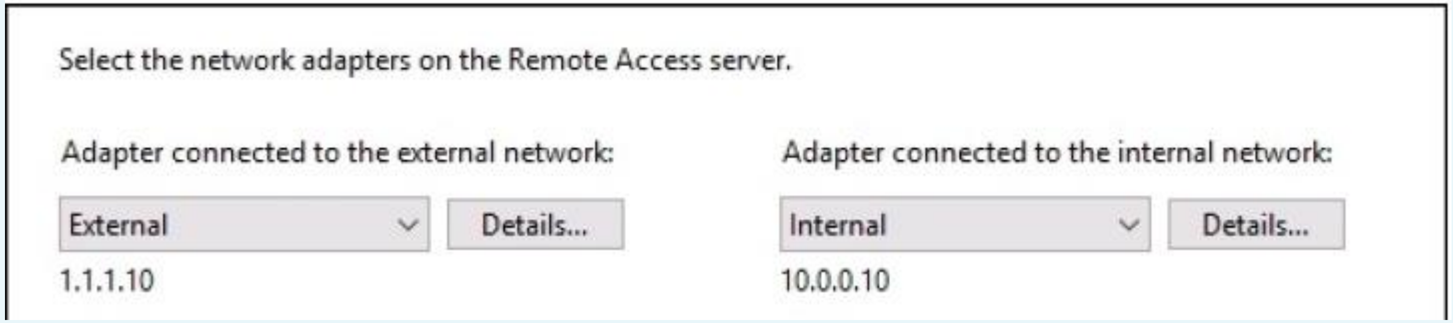
Prerequisites: one or two NICs?

- **Edge mode with two NICs:**
  - It is the way that DA works best
  - Internal NIC typically gets plugged right into the corporate network
  - External NIC's physical placement can vary depending on the organization
  - External NIC is always the one that receives the Default Gateway settings.
  - **Since this server is multihomed, you will likely need to create some route statements**

DirectAccess

Prerequisites: one or two NICs?

- **More than two NICs?**
  - DA configuration itself is only capable of managing two different network interfaces
  - During the setup wizards you will have to define one NIC as External, and the other as Internal
  - Any more NICs that exist in that server will not be used by DA



Select the network adapters on the Remote Access server.

Adapter connected to the external network: External

1.1.1.10

Adapter connected to the internal network: Internal

10.0.0.10

DirectAccess

Tunneling protocol options

- When DA laptop makes a connection to the DA server, it will use one of the three IPv6 transition tunneling protocols:
  - 6to4: Used by DA clients with a public IP address
  - Teredo: Used by DA clients with a private IP address behind a NAT device
  - IP-HTTPS: Used by DA clients if they are not able to use 6to4, or Teredo
- When establishing the tunnel, the DA client will automatically choose which of these protocols is best to use

DirectAccess

Tunneling protocol options

- **6to4:**
  - DA clients only attempt to use 6to4 when the remote laptop has a true public Internet IP address
  - This hardly ever happens these days with the shortage of available Internet IPv4 addresses
  - It is common practice to disable the 6to4 adapter on the client computers as a DA best practice setting.

DirectAccess

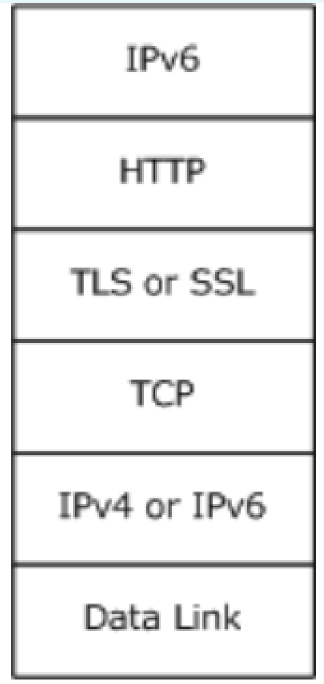
Tunneling protocol options

- **Teredo:**
  - When DA clients are connected to the Internet using a private IP address, they will attempt to connect using the Teredo protocol
  - Teredo uses a UDP stream to encapsulate these packets
  - So as long as the user's Internet connection allows outbound UDP 3544, Teredo will generally connect and be the transition protocol of choice for that DA connection.

DirectAccess

Tunneling protocol options

- IP-HTTPS (pronounced IP over HTTPS):
  - If Teredo fails to connect, e.g., blocks outbound UDP, then the DA connection will use IP-HTTPS
  - Encapsulating the IPv6 packets inside IPv4 headers, but then wraps that up inside an HTTP header and encrypts it with TLS/SSL before sending the packet out over the Internet.
  - Effectively makes the DA connection an SSL stream, just like when you browse an HTTPS website.



DirectAccess

Installing on the true edge

- Plug DA server's External NIC directly into the Internet: put true public IP addresses on that NIC
- All three of the above transition tunneling protocols are enabled: DA client can choose between them for the best form of connectivity

DirectAccess

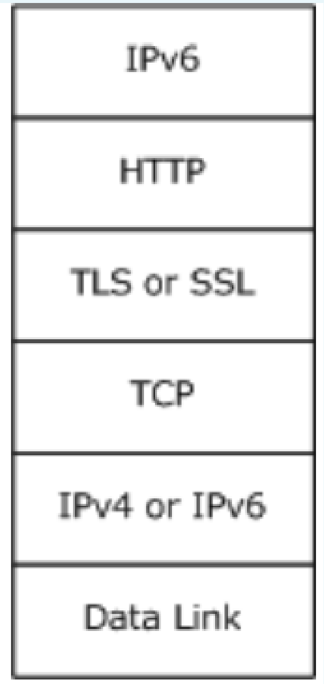
Installing behind a NAT

- It is much more common for the networking team to place the external NIC of DA server behind a firewall
- This typically means creating a NAT in order to bring this traffic into the server
- When you install a DA server behind a NAT, Teredo no longer works
- In fact, the DA configuration wizards will recognize when you have a private IP address listed on the external NIC and it will not even turn on Teredo.

DirectAccess

Installing behind a NAT

- When Teredo is not available, all of DA clients will connect using IP-HTTPS.
- Teredo:
  - more efficient protocol than IP-HTTPS because it is simply encapsulating IPv6 inside IPv4
  - no need any additional encryption because DA traffic stream is already and always IPsec encrypted



IPv6

HTTP

TLS or SSL

TCP

IPv4 or IPv6

Data Link

DirectAccess

Installing behind a NAT

- IP-HTTPS:
  - takes the already encrypted IPsec traffic stream and encrypts it a second time using SSL.
  - being subject to additional processing and CPU cycles, and it makes for a slower connection
  - creates additional hardware load on the DA server itself.
- To summarize:
  - DA server's external NIC can be behind a NAT
  - But the DA client will be connecting using the IP-HTTPS protocol, and it has the side effects of implementing in this way.

DirectAccess

Network Location Server (NLS)

- A website running inside the corporate network
- This website does not need (should not) to be available for access over the Internet
- Used as part of the inside/outside detection mechanism on the DA client computers.
- Every time a DA client gets a network connection, it starts looking for the NLS website
  - If it can see the site, then it knows that you are inside the corporate network, and DA is not required, so it turns itself off.

DirectAccess

Network Location Server

- If NLS website cannot be contacted,, i.e., the computer is outside of the corporate network, and the DA components will start turning themselves on.
- All you need to do is spin up a VM and install IIS on it to host this new website.
- Two things when setting up your NLS website:
  - It must be an HTTPS site, and so it requires an SSL certificate
  - DNS name you are using in order to contact this website is unique

DirectAccess

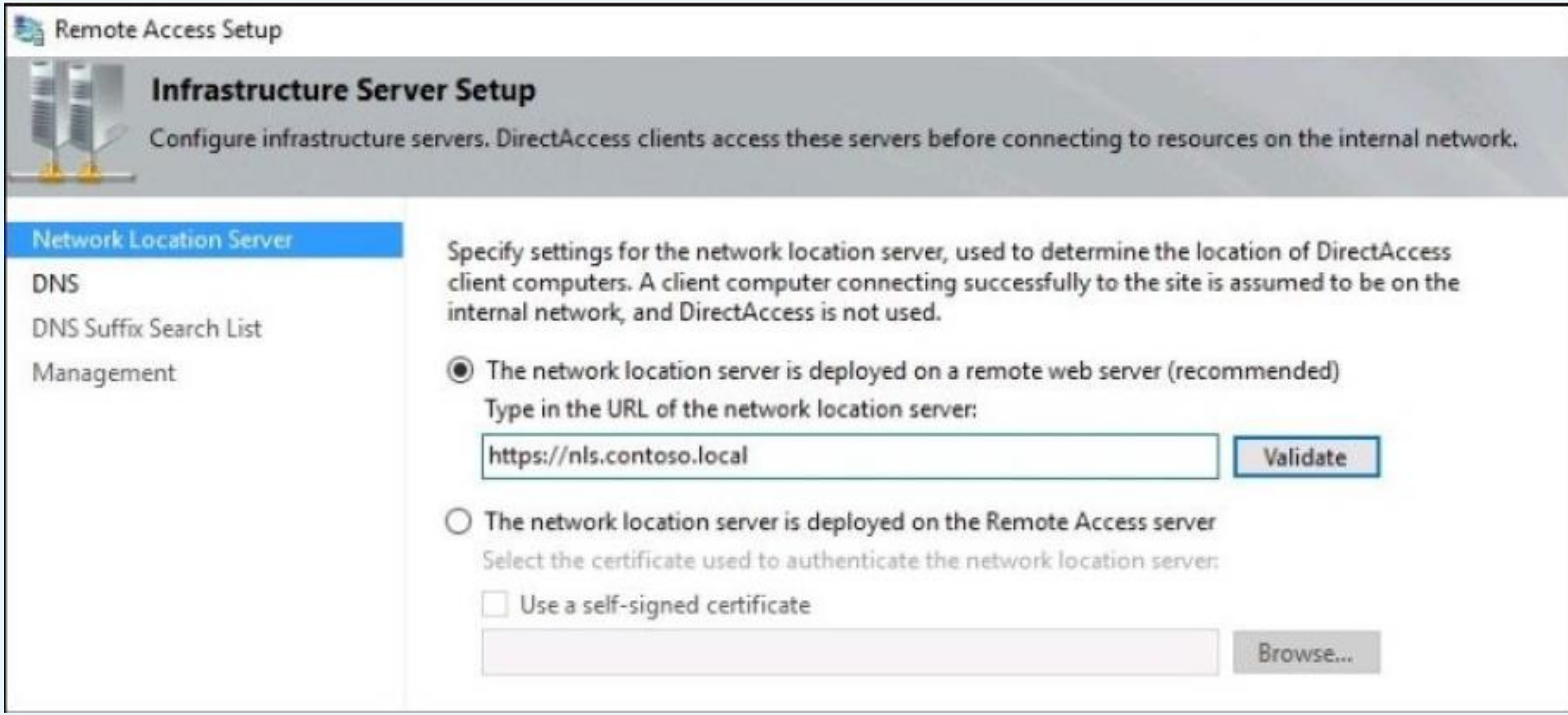
Network Location Server

- NLS **should not be implemented** on the DA server itself.
- Many things that can go wrong when you cohost NLS on the DA server
- Running NLS on your DA server also limits the DA potential in the future
- Some of the advanced DA configurations require to remove NLS from the DA server anyway

DirectAccess

Network Location Server

DA config wizards to choose the location of NLS



Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.

● The network location server is deployed on a remote web server (recommended)

Type in the URL of the network location server:

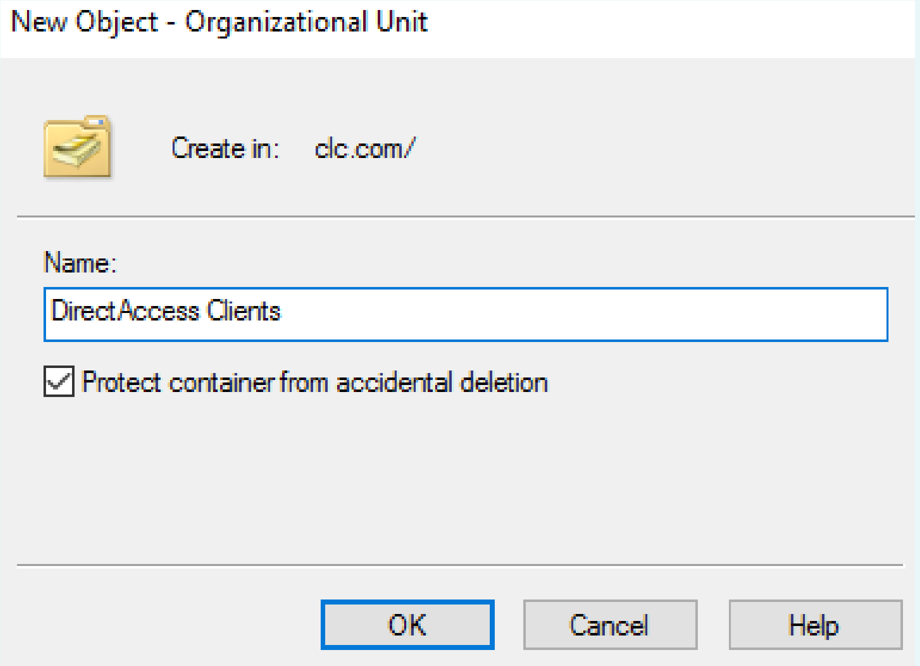
https://nls.contoso.local

○ The network location server is deployed on the Remote Access server

Select the certificate used to authenticate the network location server:

□ Use a self-signed certificate

- Creating DA OU & Group in Active Directory:



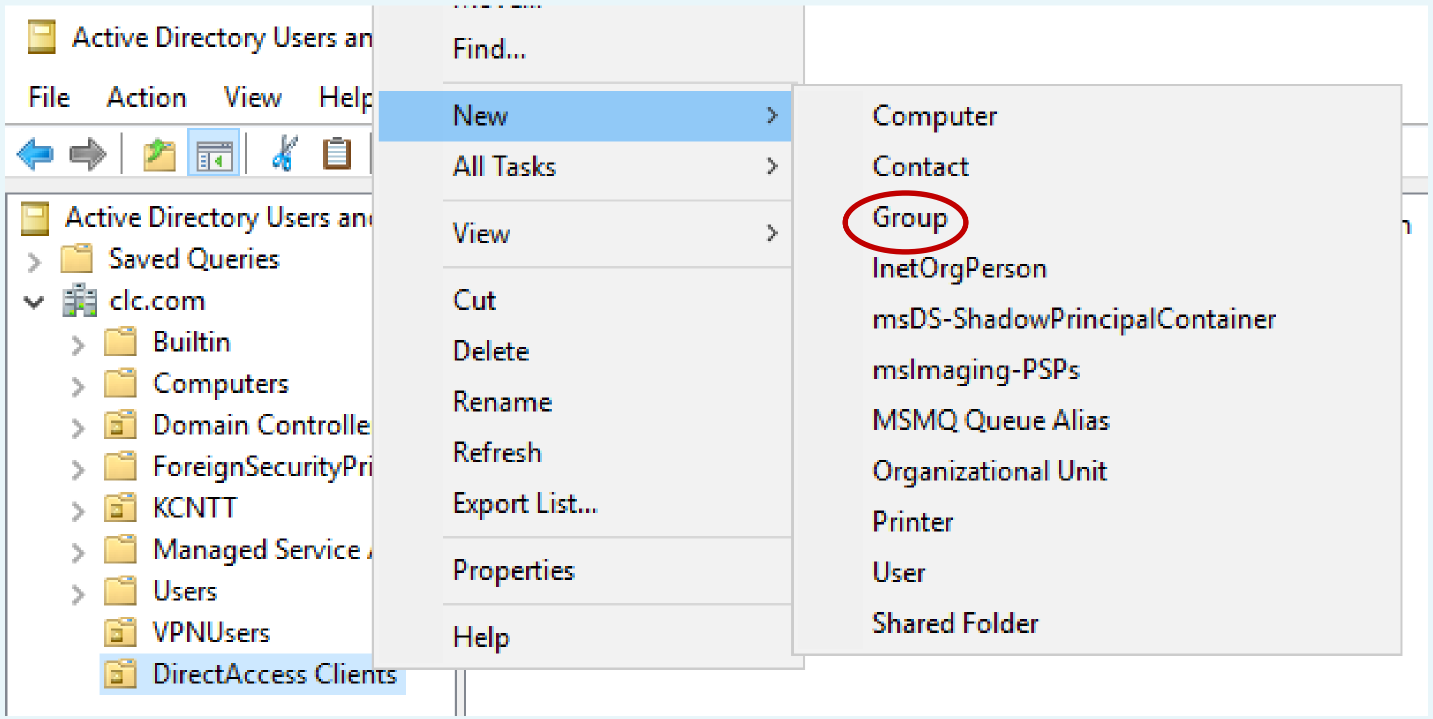
New Object - Organizational Unit

Create in: clc.com/

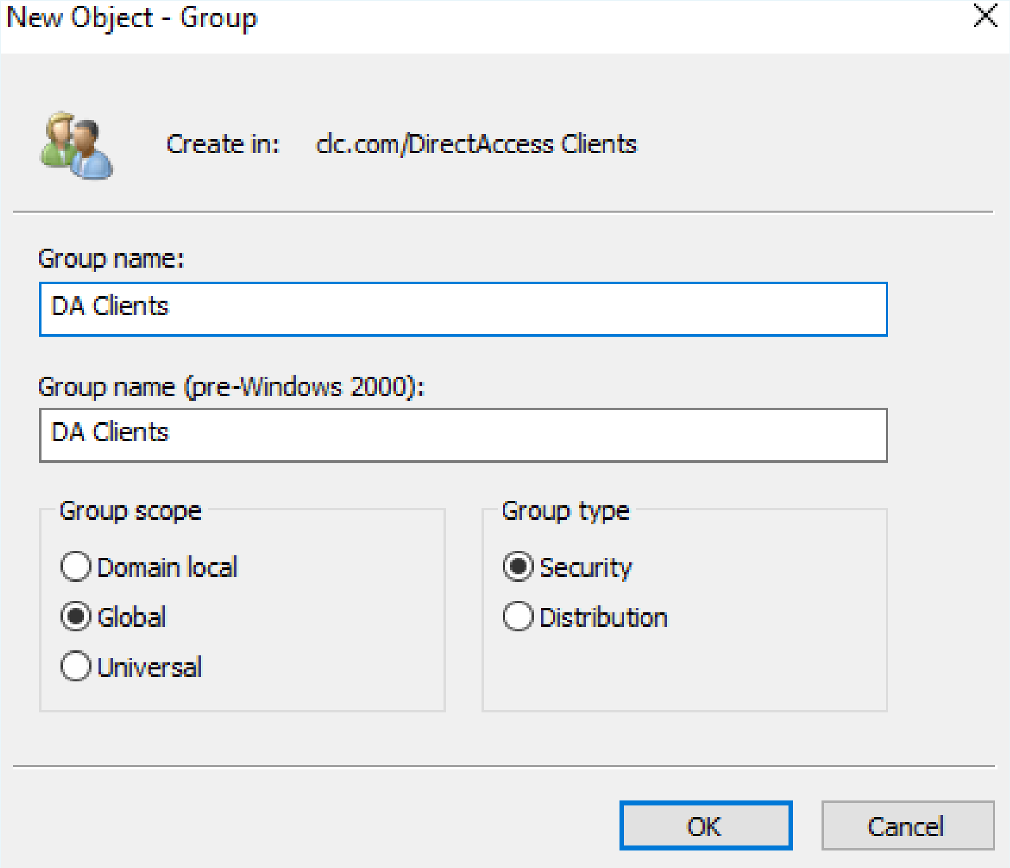
Name:

DirectAccess Clients

☑ Protect container from accidental deletion



- Creating DA OU & Group in Active Directory:



New Object - Group

Create in: dlc.com/DirectAccess Clients

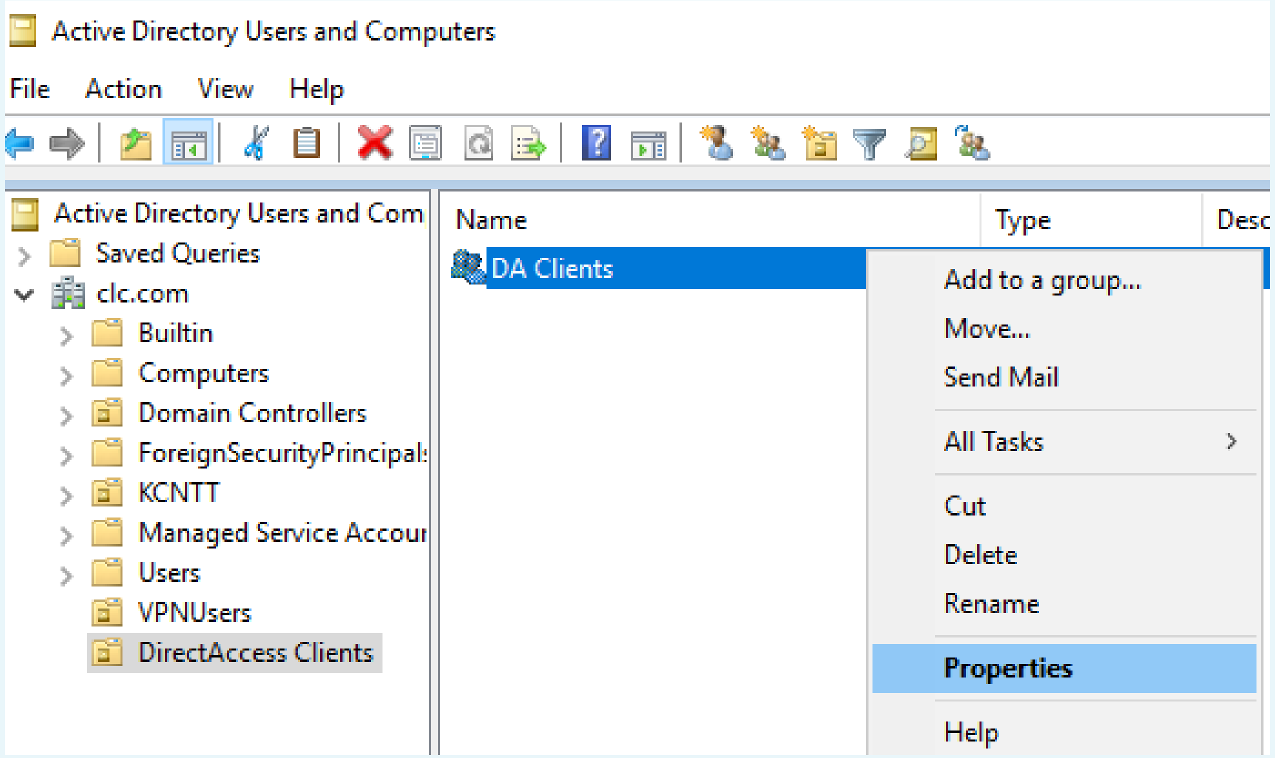
Group name:
DA Clients

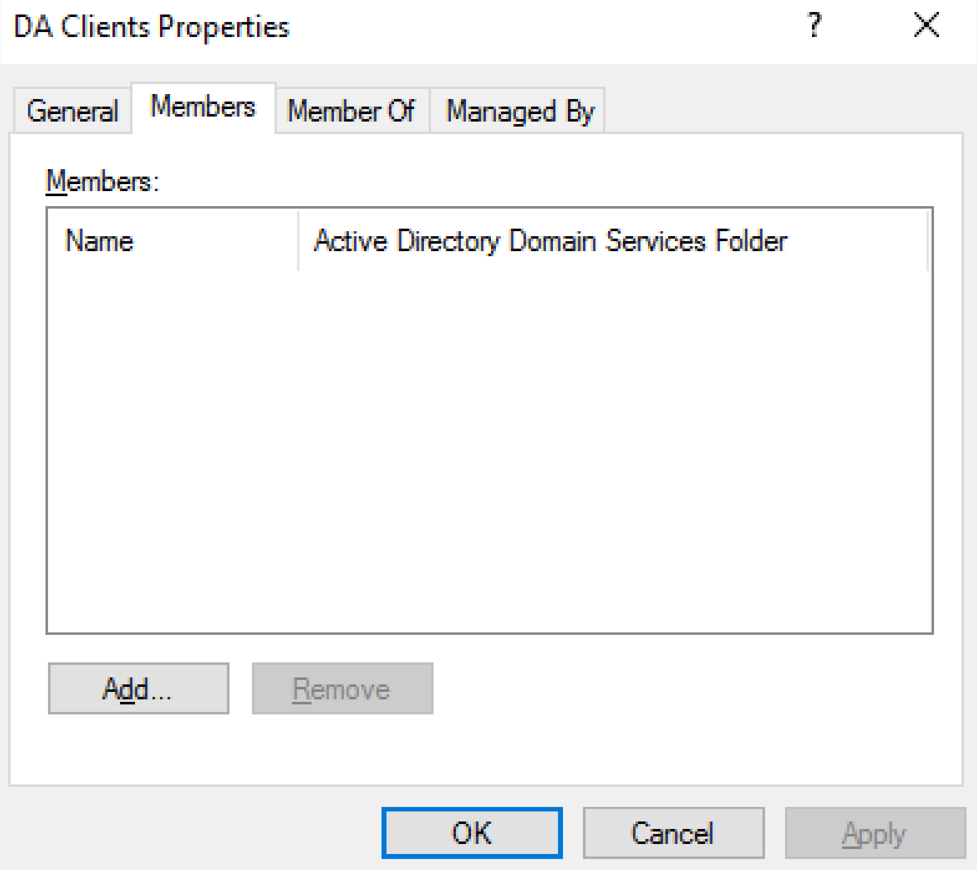
Group name (pre-Windows 2000):
DA Clients

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

- Creating DA OU & Group in Active Directory:

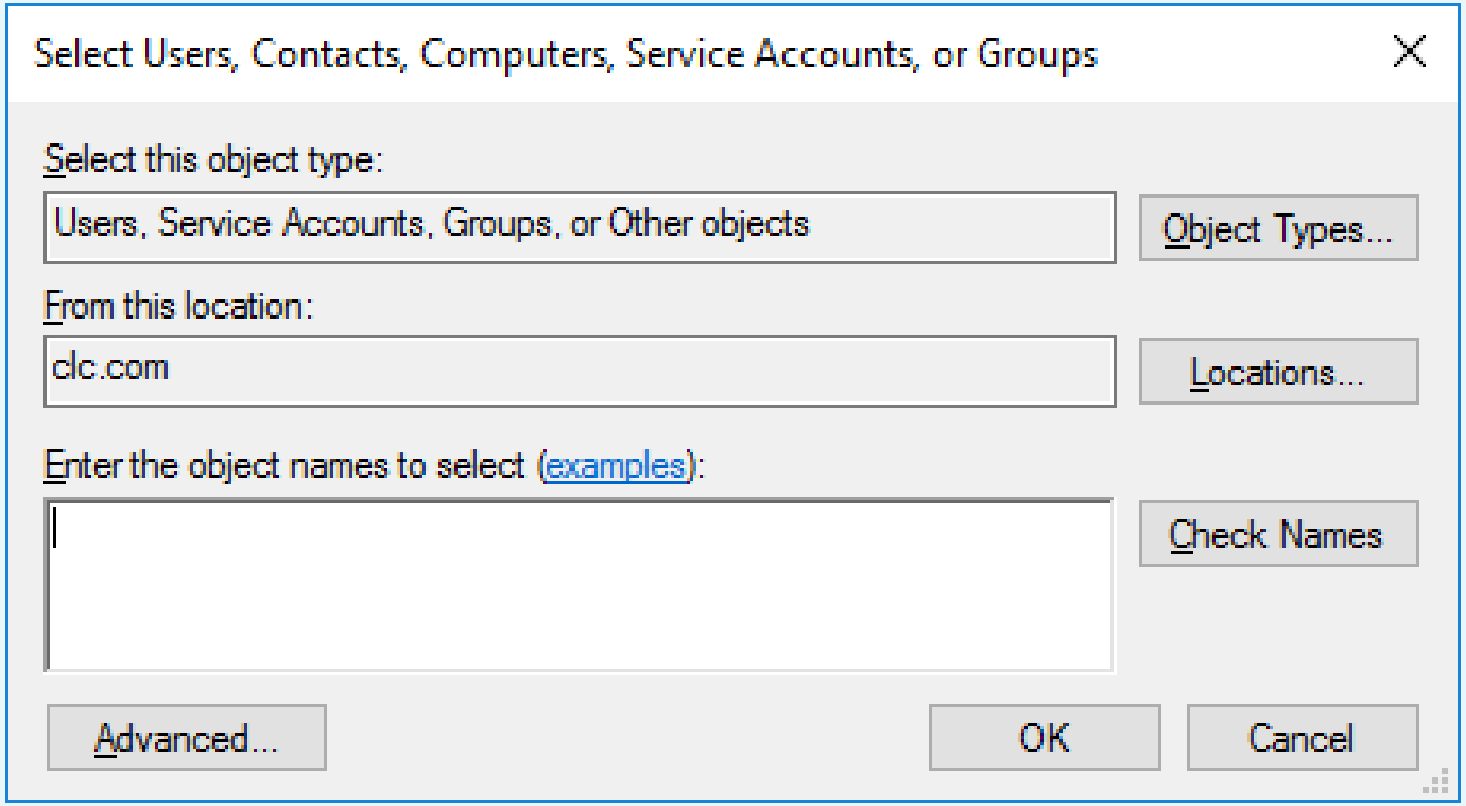




DirectAccess

Install and configure

- Creating DA OU & Group in Active Directory:



Select Users, Contacts, Computers, Service Accounts, or Groups

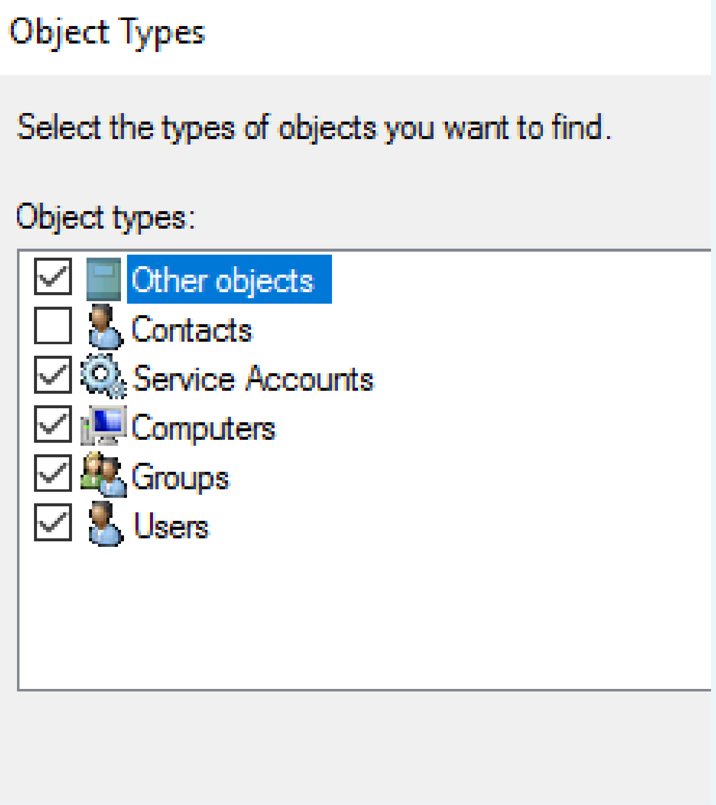
Select this object type:

Users, Service Accounts, Groups, or Other objects

From this location:

clc.com

Enter the object names to select (examples):



Object Types

Select the types of objects you want to find.

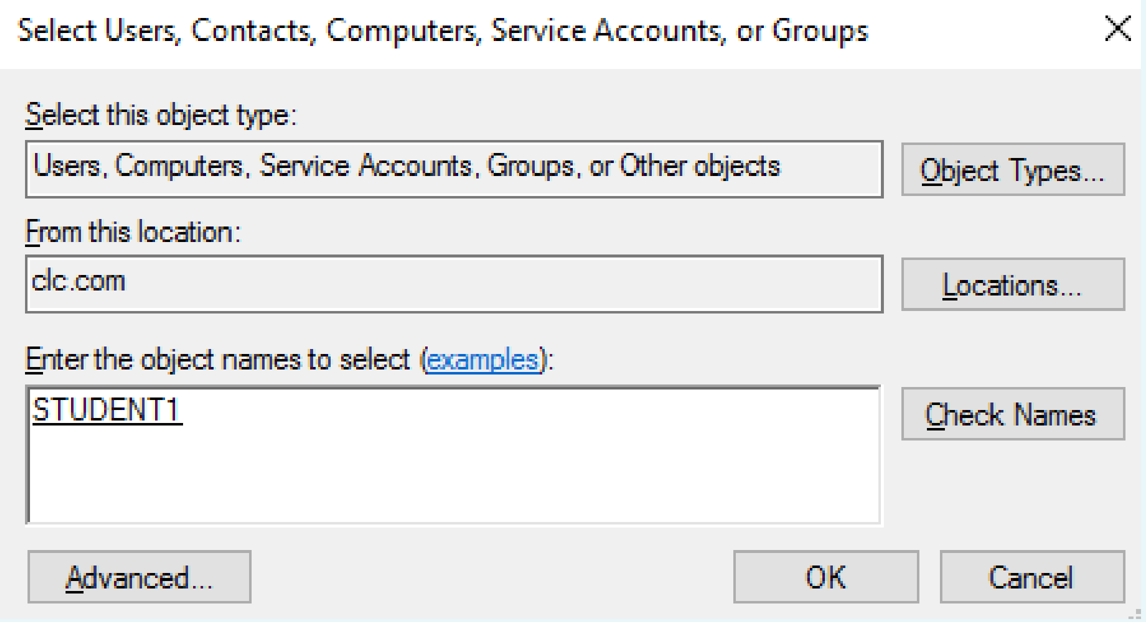
Object types:

- ☑ Other objects
- □ Contacts
- ☑ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

DirectAccess

Install and configure

- Creating DA OU & Group in Active Directory:

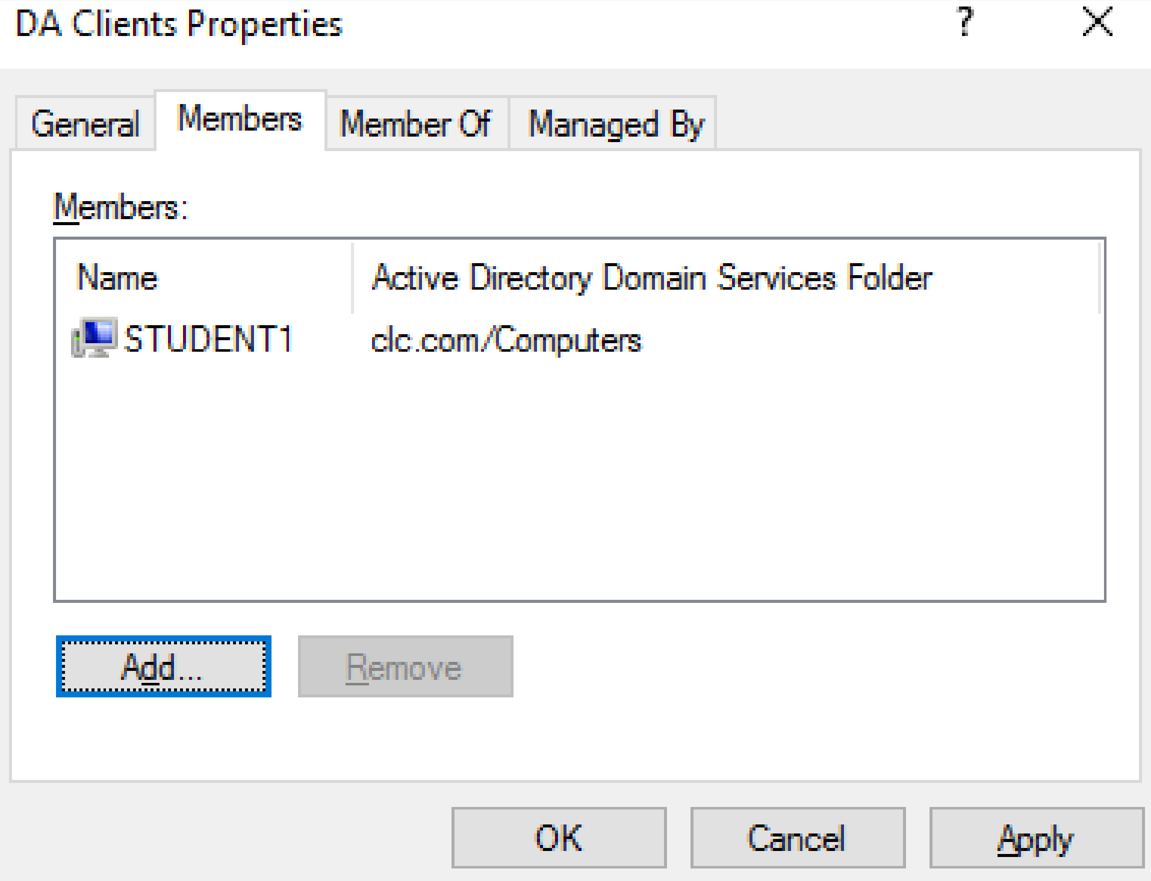


Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type: Users, Computers, Service Accounts, Groups, or Other objects

From this location: clc.com

Enter the object names to select (examples): STUDENT1



DA Clients Properties

Members:

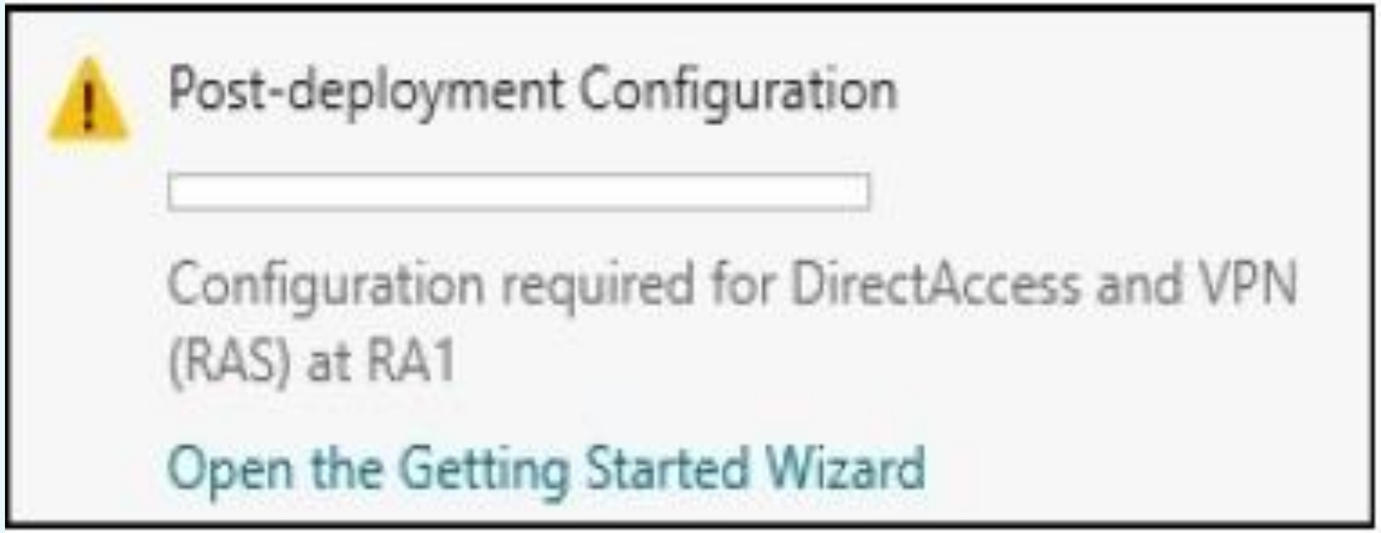
Name	Active Directory Domain Services Folder
STUDENT1	clc.com/Computers

DirectAccess

Install and configure

- The network model for DA is the same as that of VPN described in previous section
- The Installation progress is also the same!!!
- After finished installing the role, you need additional configuration

- Donot follow the yellow exclamation mark inside Server Manager as with configuring VPN



Post-deployment Configuration

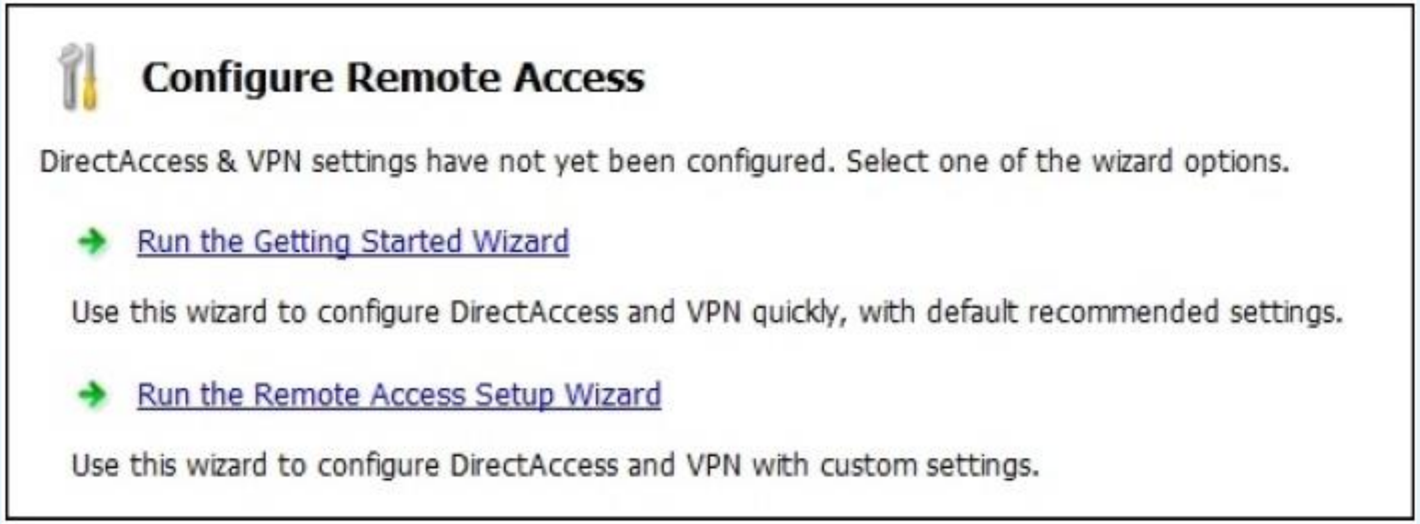
Configuration required for DirectAccess and VPN (RAS) at RA1

Open the Getting Started Wizard

DirectAccess

Install and configure

- To configure DA: use the **Remote Access Management Console** (Server Manager ->Tool)



Configure Remote Access

DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.

→ Run the Getting Started Wizard

Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.

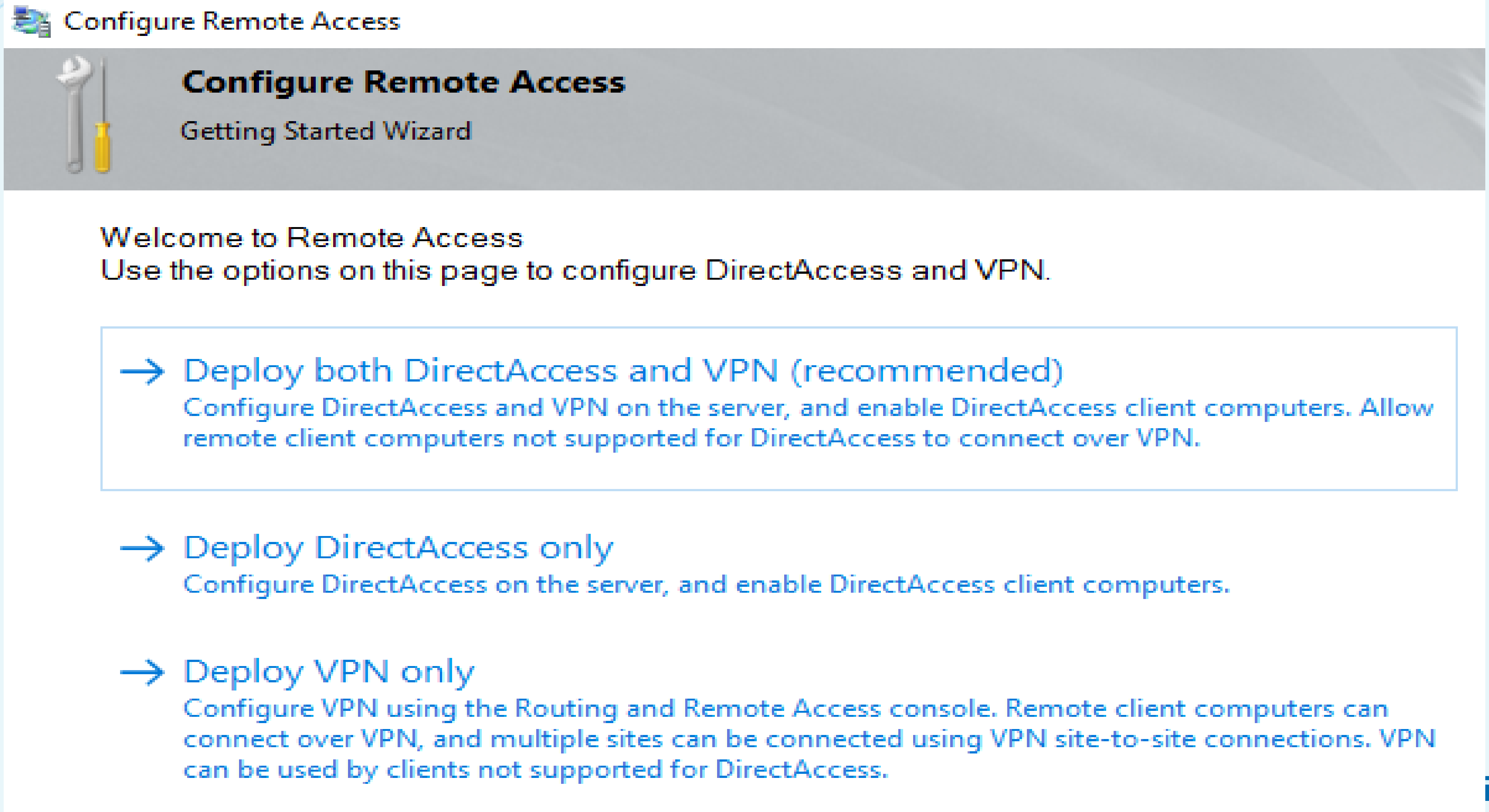
→ Run the Remote Access Setup Wizard

Use this wizard to configure DirectAccess and VPN with custom settings.

- Click on the Getting Started Wizard

DirectAccess

Install and configure



Configure Remote Access

Configure Remote Access

Getting Started Wizard

Welcome to Remote Access
Use the options on this page to configure DirectAccess and VPN.

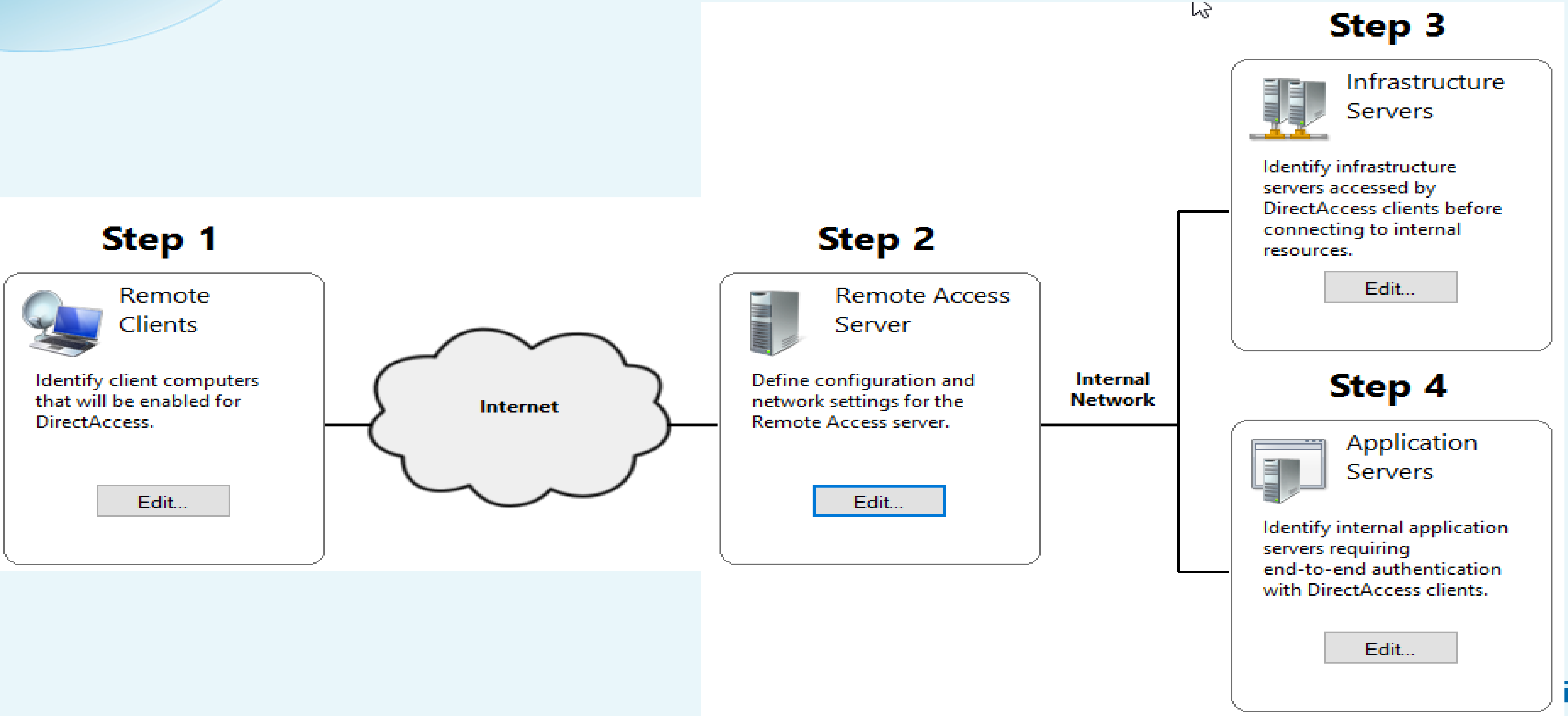
→ Deploy both DirectAccess and VPN (recommended)
Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.

→ Deploy DirectAccess only
Configure DirectAccess on the server, and enable DirectAccess client computers.

→ Deploy VPN only
Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.

DirectAccess

Install and configure



Step 1

Remote Clients

Identify client computers that will be enabled for DirectAccess.

Step 2

Remote Access Server

Define configuration and network settings for the Remote Access server.

Step 3

Infrastructure Servers

Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

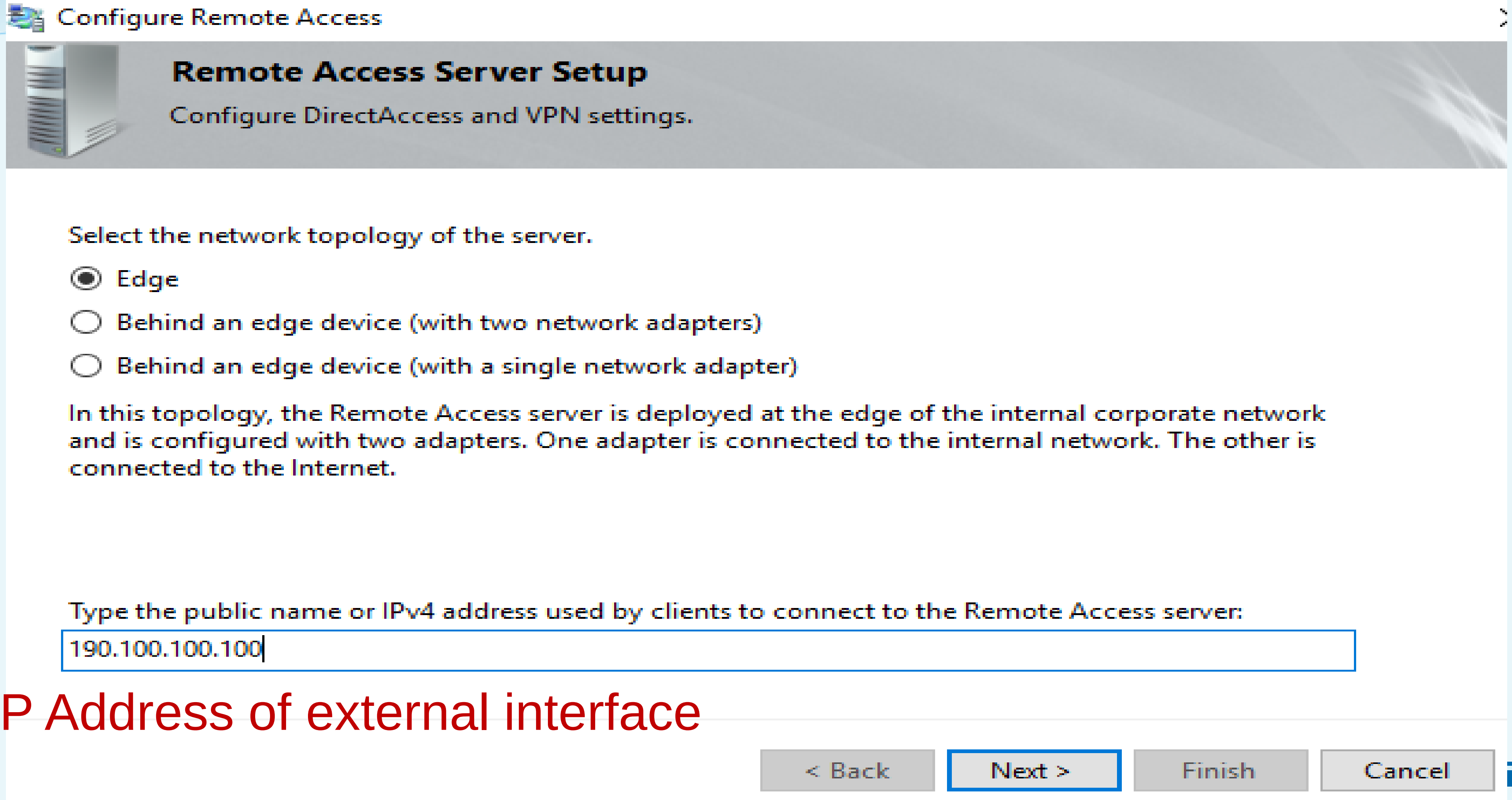
Step 4

Application Servers

Identify internal application servers requiring end-to-end authentication with DirectAccess clients.

DirectAccess

Install and configure



Configure Remote Access

Remote Access Server Setup

Configure DirectAccess and VPN settings.

Select the network topology of the server.

● Edge

○ Behind an edge device (with two network adapters)

○ Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

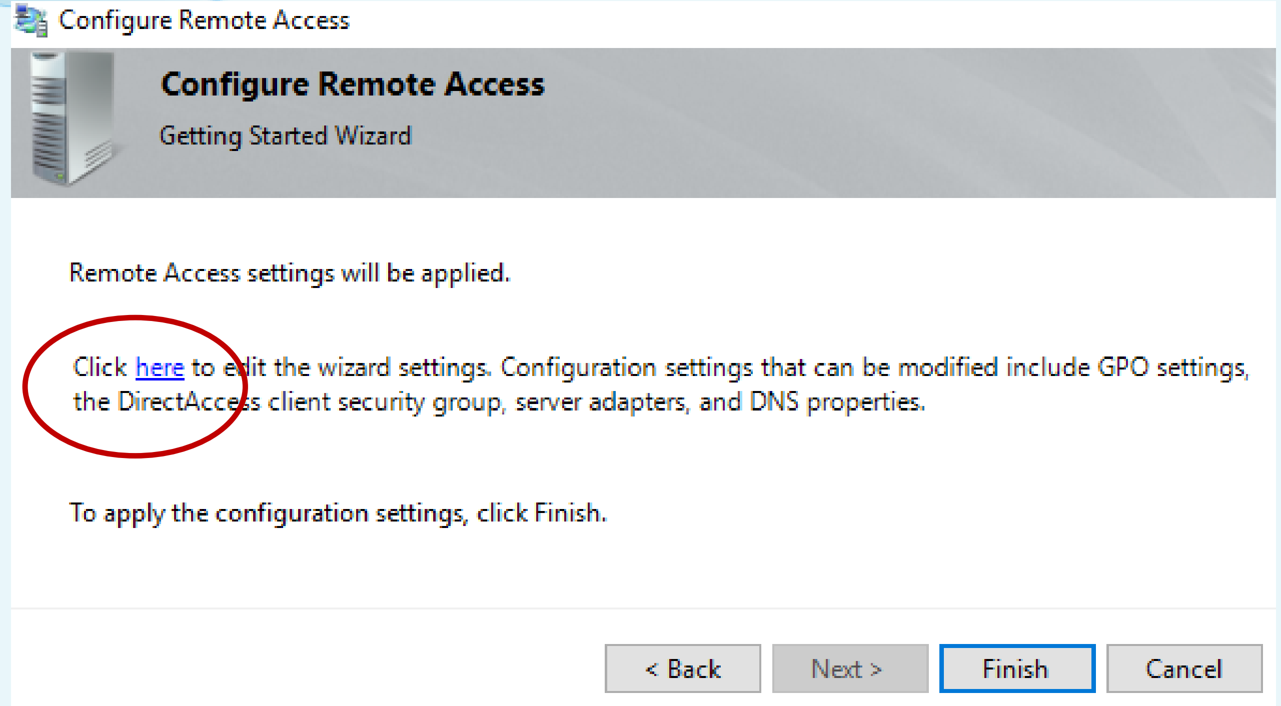
Type the public name or IPv4 address used by clients to connect to the Remote Access server:

190.100.100.100

IP Address of external interface

DirectAccess

Install and configure



Configure Remote Access

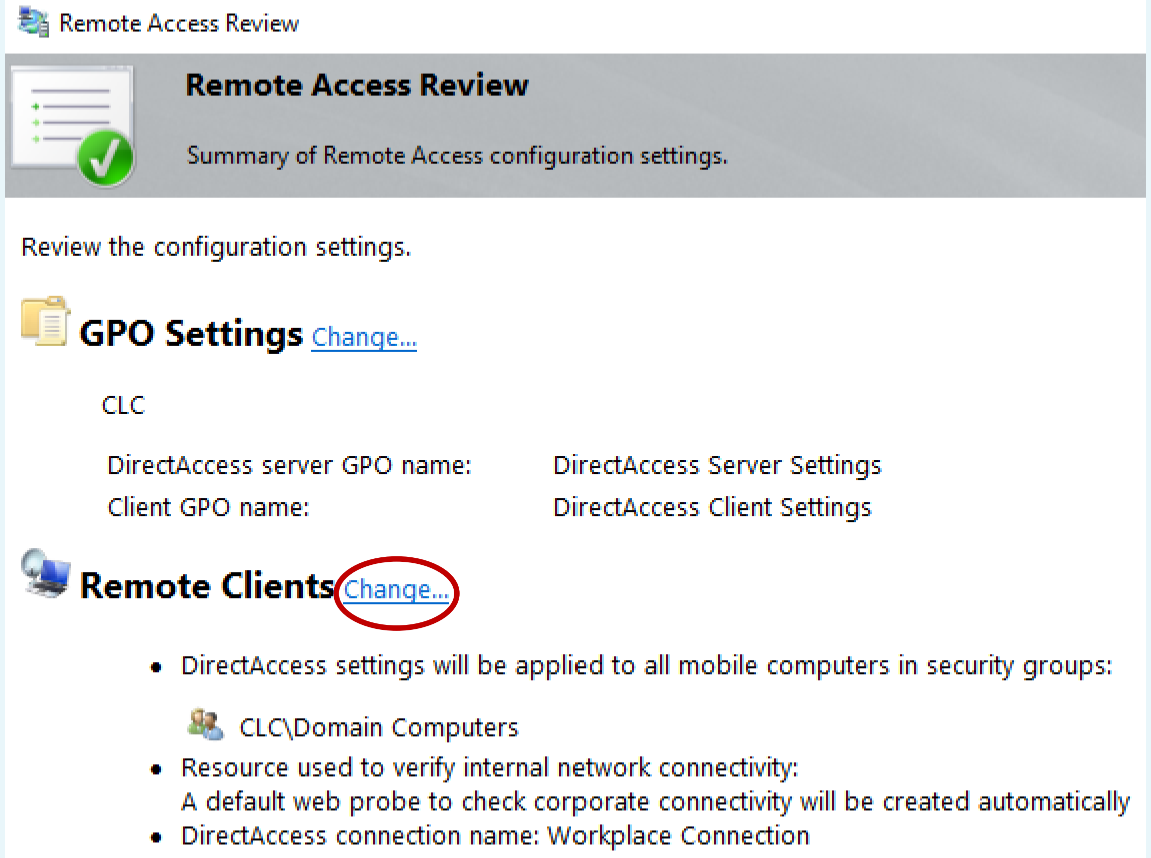
Configure Remote Access

Getting Started Wizard

Remote Access settings will be applied.

Click here to edit the wizard settings. Configuration settings that can be modified include GPO settings, the DirectAccess client security group, server adapters, and DNS properties.

To apply the configuration settings, click Finish.



Remote Access Review

Remote Access Review

Summary of Remote Access configuration settings.

Review the configuration settings.

GPO Settings Change...

CLC

DirectAccess server GPO name:	DirectAccess Server Settings
Client GPO name:	DirectAccess Client Settings

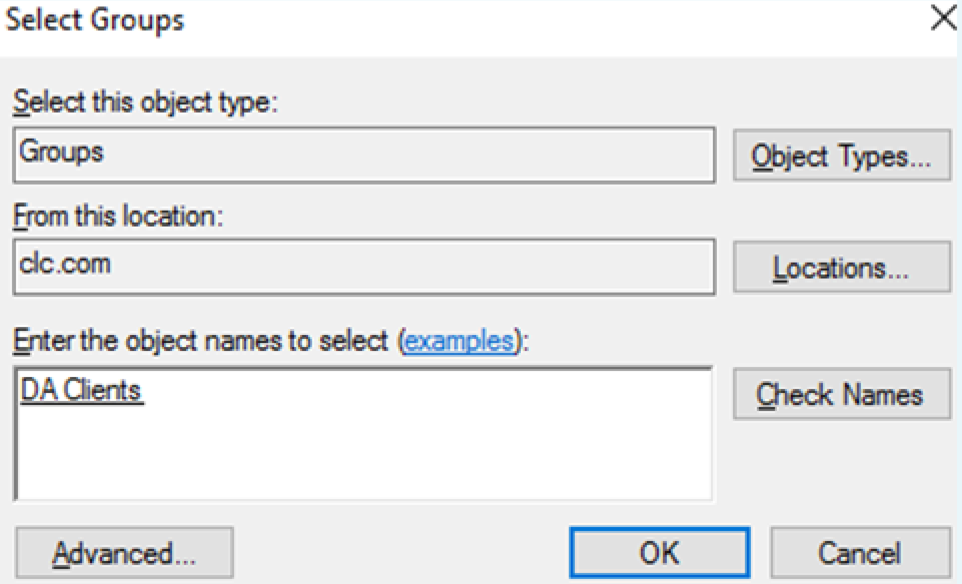
Remote Clients Change...

- DirectAccess settings will be applied to all mobile computers in security groups:

  CLC\Domain Computers
- Resource used to verify internal network connectivity:
  A default web probe to check corporate connectivity will be created automatically
- DirectAccess connection name: Workplace Connection

DirectAccess

Install and configure



Select Groups

Select this object type:

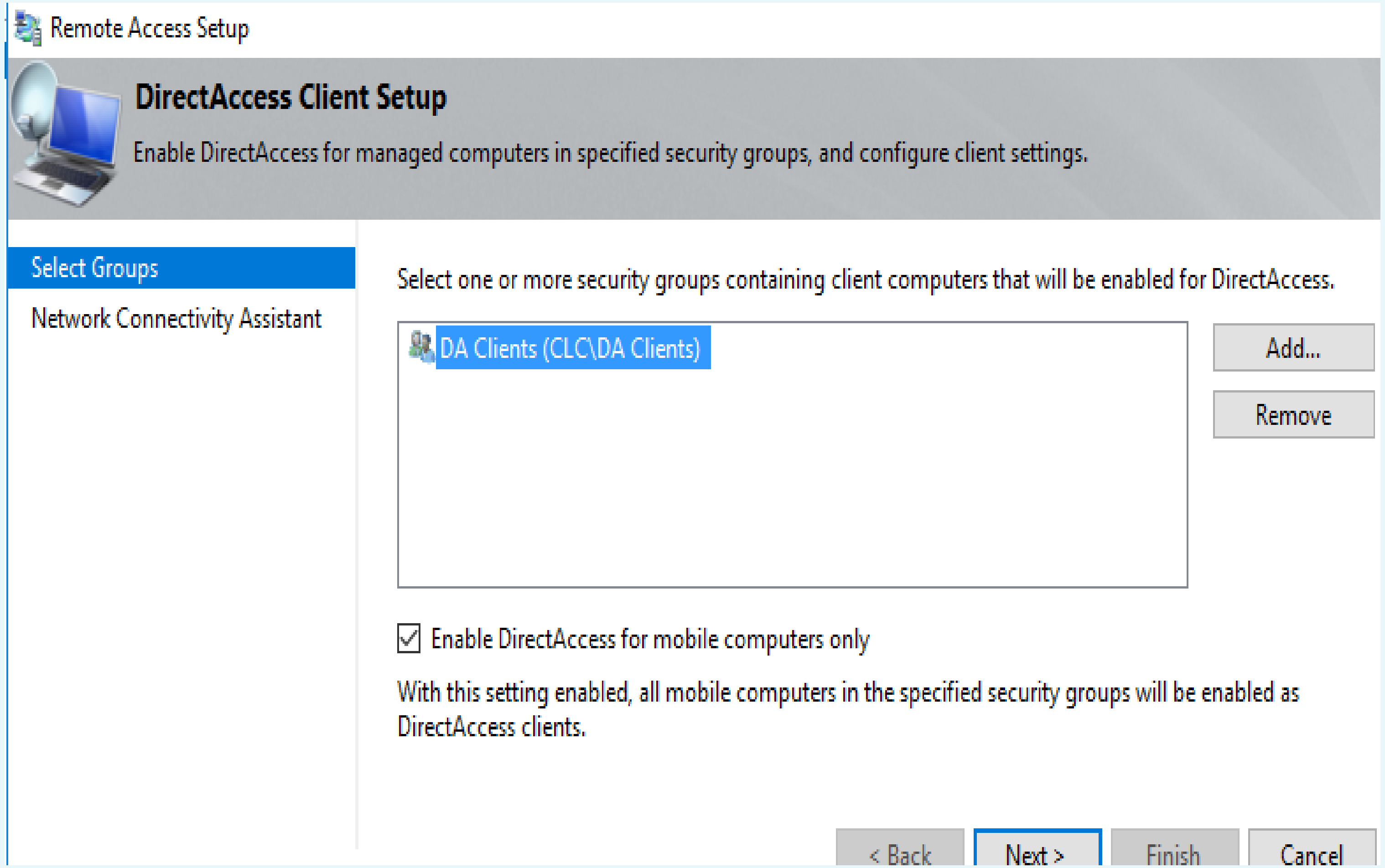
Groups

From this location:

clc.com

Enter the object names to select (examples):

DA Clients



Remote Access Setup

DirectAccess Client Setup

Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Select one or more security groups containing client computers that will be enabled for DirectAccess.

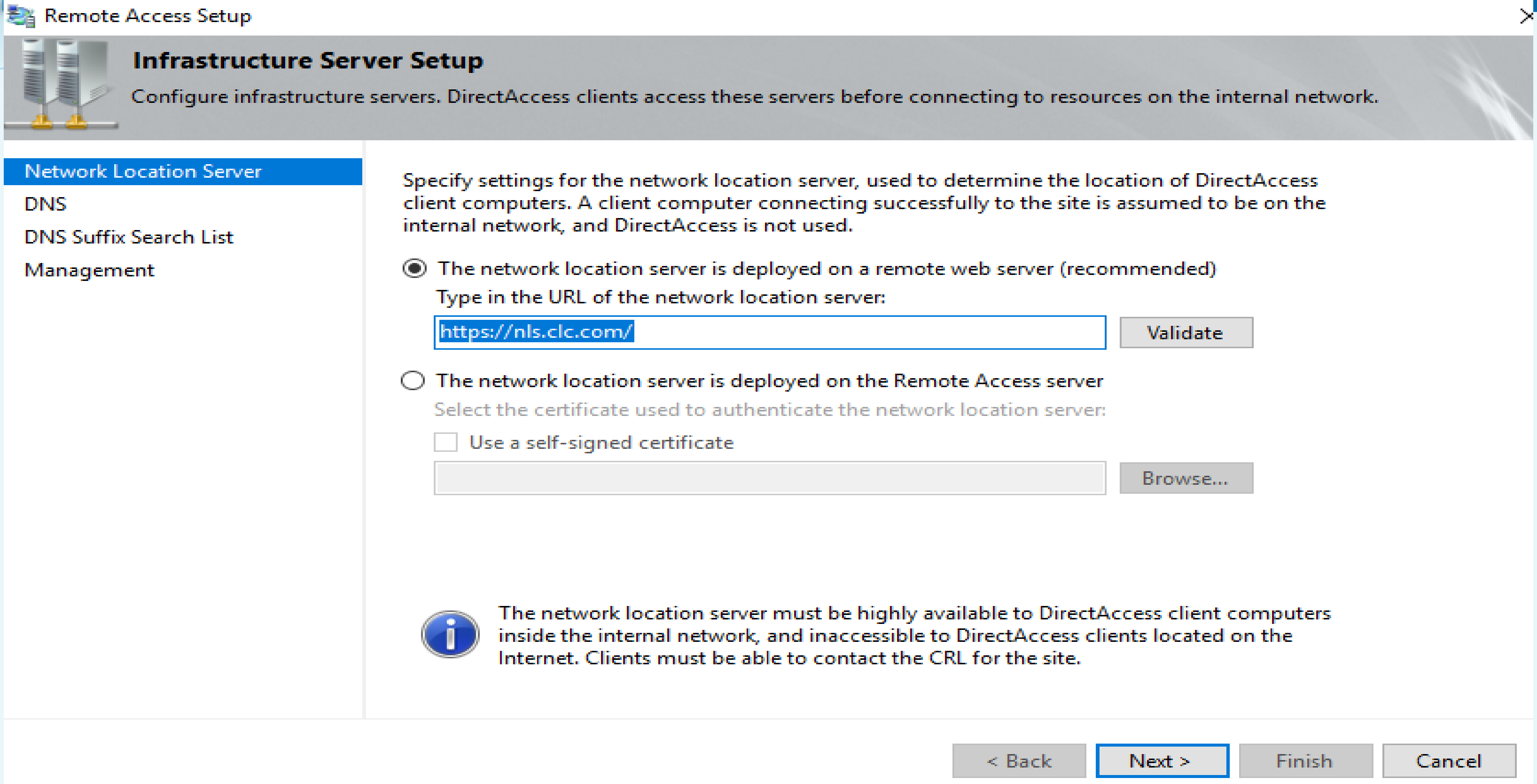
DA Clients (CLC\DA Clients)

☑ Enable DirectAccess for mobile computers only

With this setting enabled, all mobile computers in the specified security groups will be enabled as DirectAccess clients.

DirectAccess

Install and configure



Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.

● The network location server is deployed on a remote web server (recommended)

Type in the URL of the network location server:

https://nls.clc.com/

○ The network location server is deployed on the Remote Access server

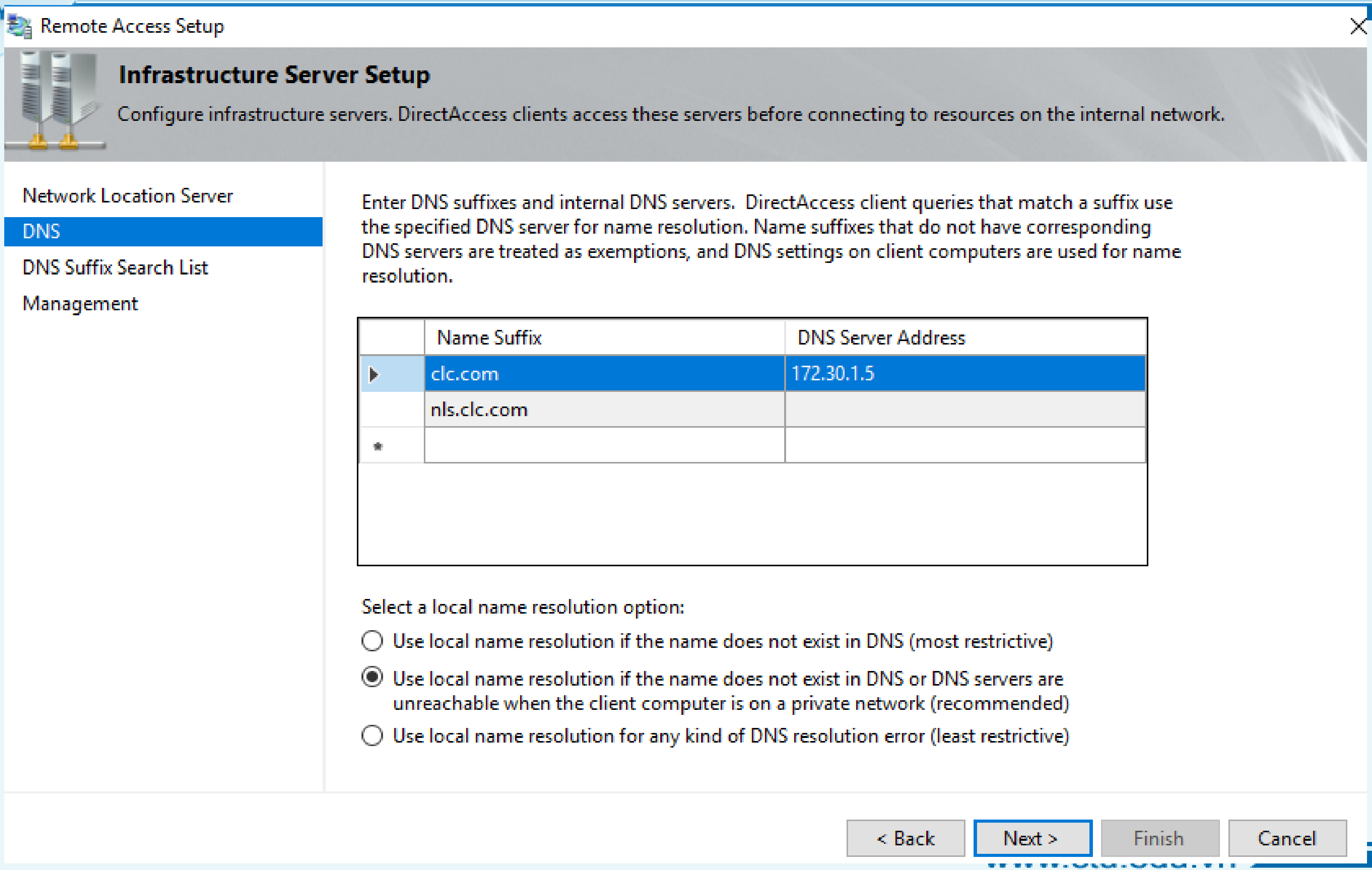
Select the certificate used to authenticate the network location server:

□ Use a self-signed certificate

The network location server must be highly available to DirectAccess client computers inside the internal network, and inaccessible to DirectAccess clients located on the Internet. Clients must be able to contact the CRL for the site.

DirectAccess

Install and configure



Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

	Name Suffix	DNS Server Address
▸	clc.com	172.30.1.5
	nls.clc.com	
*		

Select a local name resolution option:

○ Use local name resolution if the name does not exist in DNS (most restrictive)

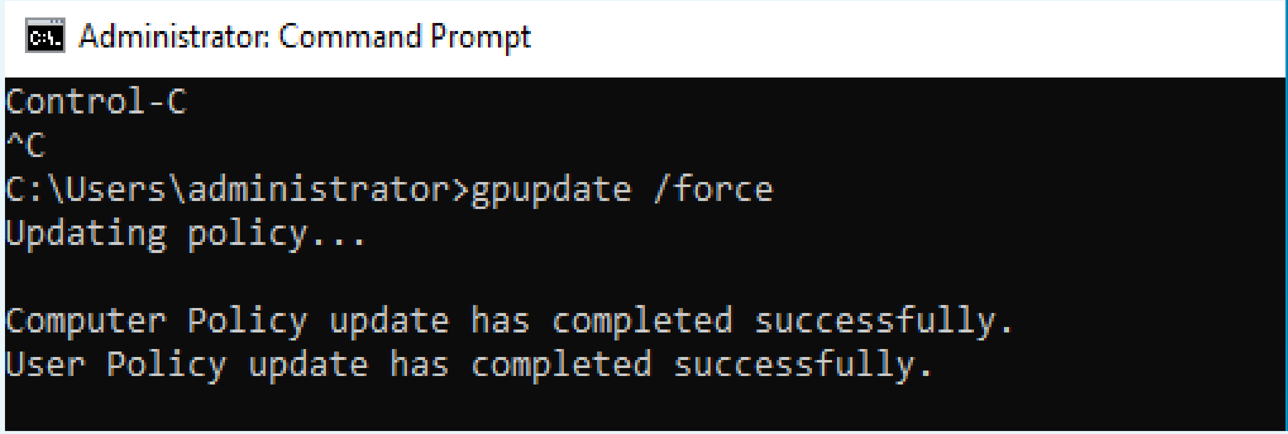
● Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)

○ Use local name resolution for any kind of DNS resolution error (least restrictive)

DirectAccess

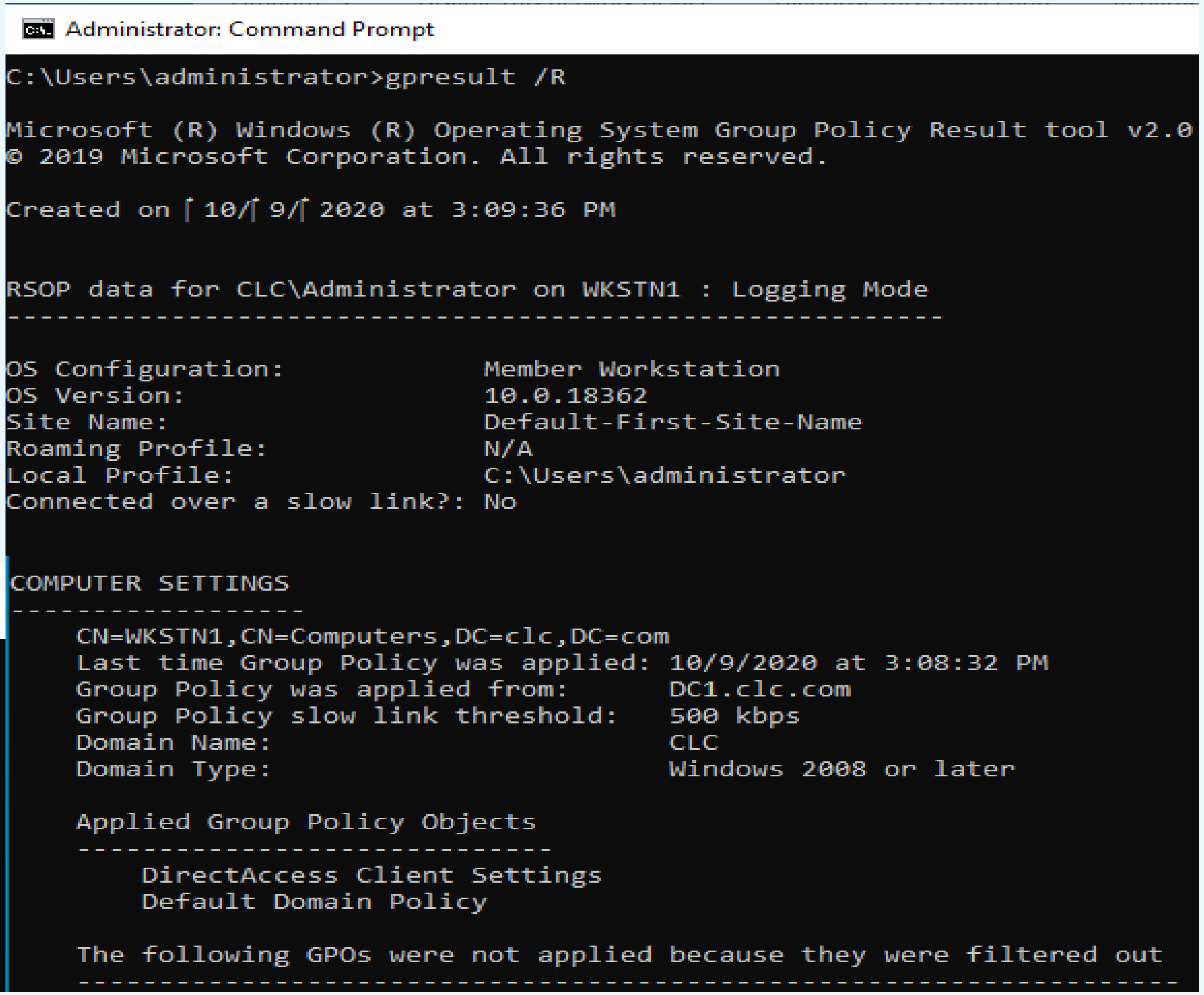
Configure the client

- Switch to CLIENT
- Verify that DirectAccessClient GPO applied to the client



Administrator: Command Prompt

```
Control-C
^C
C:\Users\administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```



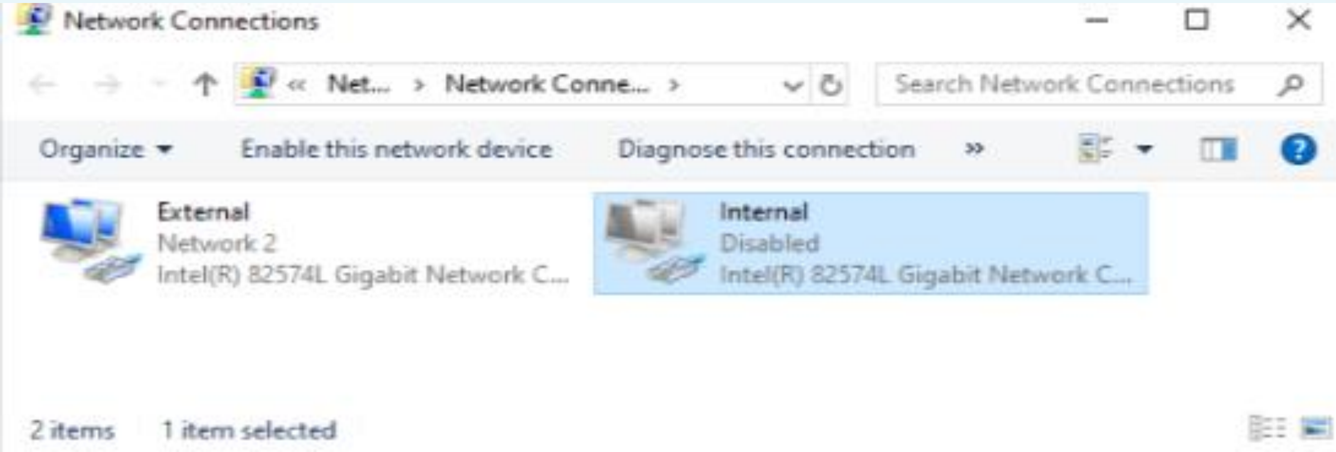
Administrator: Command Prompt

```
C:\Users\administrator>gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2019 Microsoft Corporation. All rights reserved.

Created on ⌈10/⌈9/⌈2020 at 3:09:36 PM


RSOP data for CLC\Administrator on WKSTN1 : Logging Mode
---------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.18362
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=WKSTN1,CN=Computers,DC=clc,DC=com
    Last time Group Policy was applied: 10/9/2020 at 3:08:32 PM
    Group Policy was applied from:      DC1.clc.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        CLC
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        DirectAccess Client Settings
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
```

DirectAccess

Configure the client

- Move the CLIENT to the Internet



Network Connections

Net... › Network Conne... ›

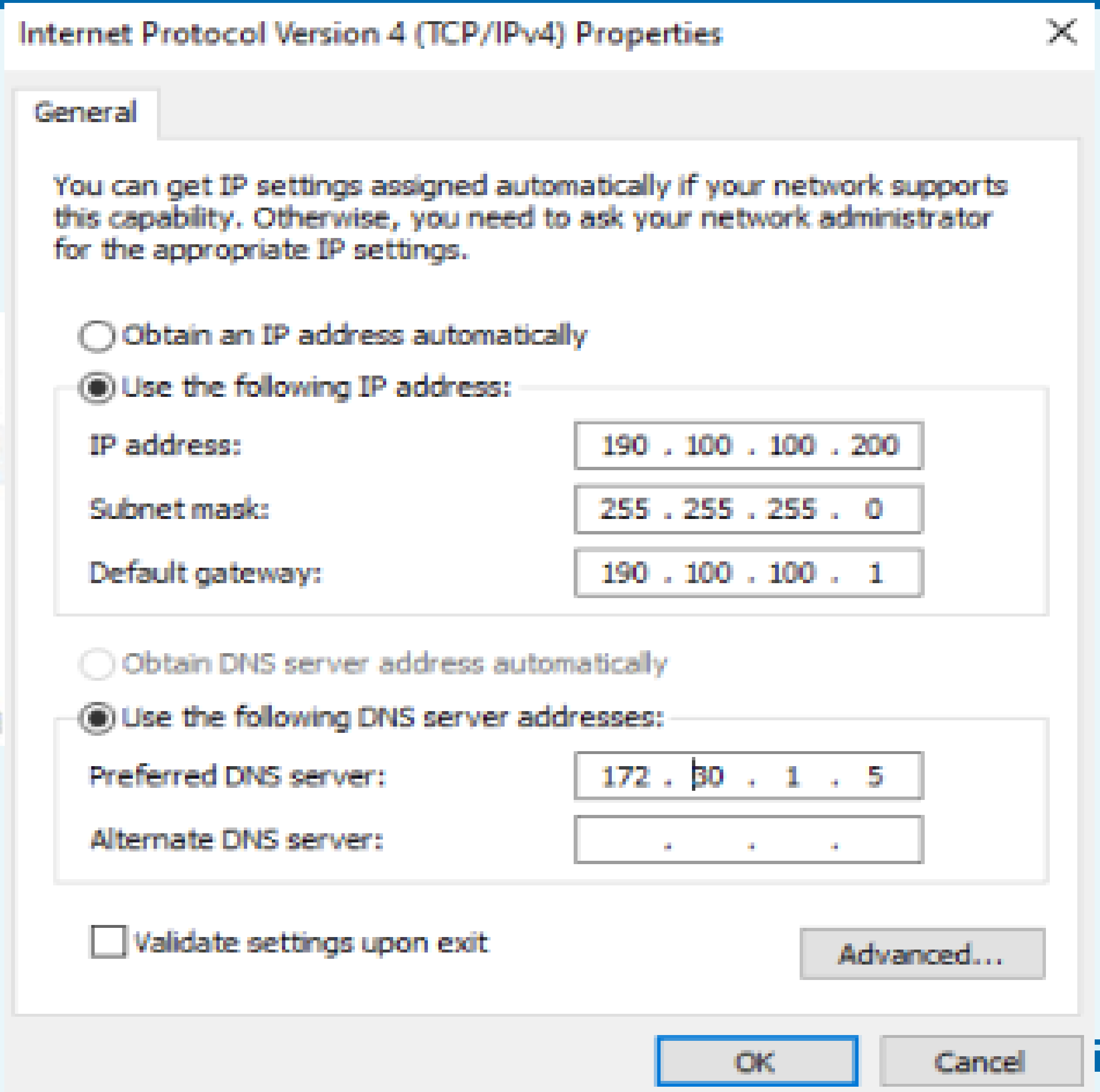
Search Network Connections

Organize ▾ Enable this network device Diagnose this connection »

External
Network 2
Intel(R) 82574L Gigabit Network C...

Internal
Disabled
Intel(R) 82574L Gigabit Network C...

2 items 1 item selected



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 190 . 100 . 100 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 190 . 100 . 100 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 30 . 1 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

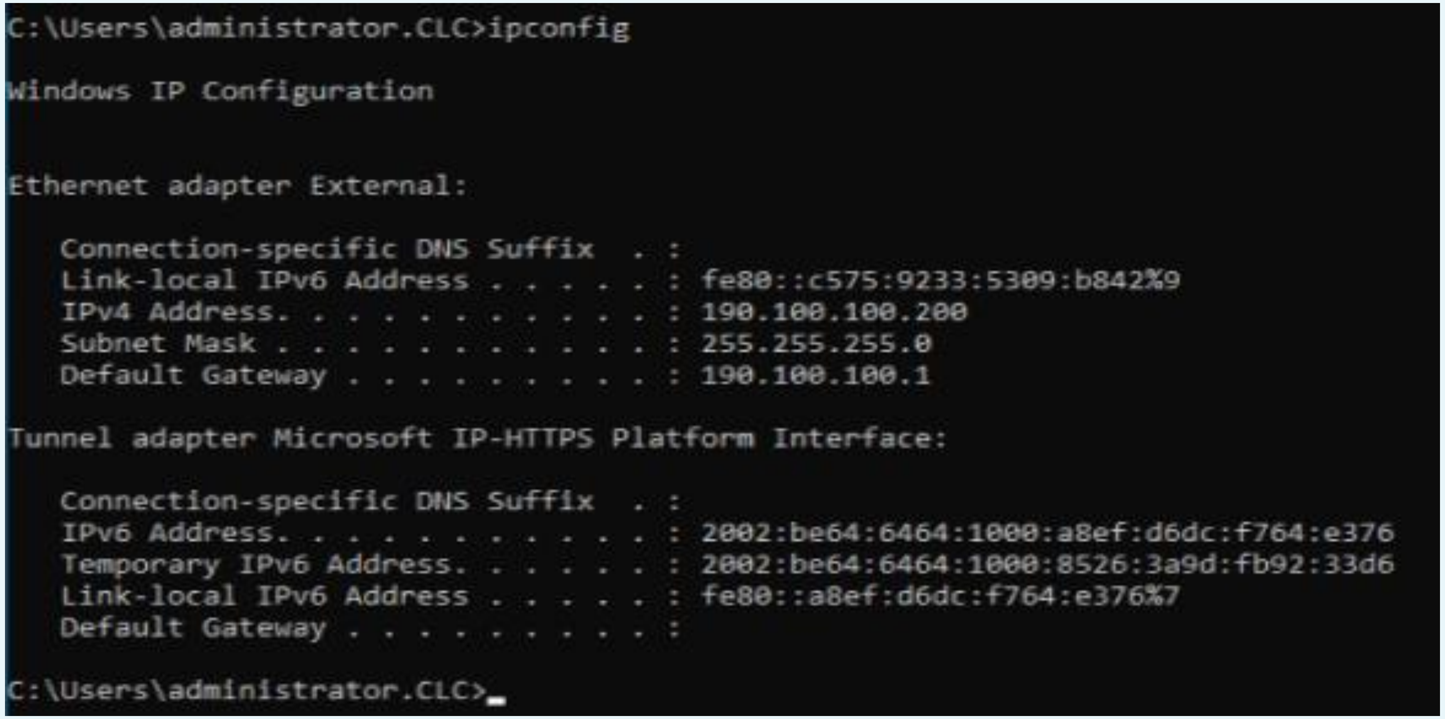
OK Cancel

DirectAccess

Configure the client

- Verify connectivity to the DirectAccess server:

  Login to DC with an account that not login using this client computer



```
C:\Users\administrator.CLC>ipconfig

Windows IP Configuration


Ethernet adapter External:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c575:9233:5309:b842%9
   IPv4 Address. . . . . . . . . . . : 190.100.100.200
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 190.100.100.1

Tunnel adapter Microsoft IP-HTTPS Platform Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:be64:6464:1000:a8ef:d6dc:f764:e376
   Temporary IPv6 Address. . . . . . : 2002:be64:6464:1000:8526:3a9d:fb92:33d6
   Link-local IPv6 Address . . . . . : fe80::a8ef:d6dc:f764:e376%7
   Default Gateway . . . . . . . . . :

C:\Users\administrator.CLC>_
```

DirectAccess versus VPN

DirectAccess versus VPN

- VPN has been around for a very long time and DirectAccess brings the speed for remote access.
- Which solutions is better for enabling your mobile workforce?
- Each has its pros and cons, and the ways that you use each, or both, will depend upon:
    - Your users, client computers, and organization's individual needs

DirectAccess versus VPN

Domain-joined versus non-domain-joined

- DirectAccess: client computer must be domain joined.
- Trusting a computer enough to be joined to your domain means that the laptop is owned by the company
- DA not ideal for situations where employees use their existing home computers to connect into work remotely
- For home and personally-owned computers, VPN may be better suited to the task

DirectAccess versus VPN

Domain-joined versus non-domain-joined

- VPN: connected from a non-domain-joined machine, and non-Microsoft devices.
  - IOS, Android, Windows Phone have a VPN client built into them.
- DirectAccess: not be able to provide non-domain-joined devices with a connectivity platform.

DirectAccess versus VPN

Auto versus manual launch

- With VPN:
  - Users have to log in to their computers to unlock them
  - Then launch the VPN
  - Then log in again to that VPN software
- With DirectAccess:
  - All they need to do is log in to the computer to unlock the screen.

DirectAccess versus VPN

Software versus built-in

- VPN:
  - Is a software
  - Needs installation, configuration, updates and maintenance
- DirectAccess:
  - Is a built-in (inside the operating system)
  - no software to install, no software to update, no software to reinstall when it breaks.
  - Everything that DA needs is already in Windows, you just aren't using it.

DirectAccess versus VPN

Password and login issues with VPN

- VPN needs to login using password
  - Sometimes the user forgets their password
- DirectAccess doesn't have these kinds of problems!
  - DA is part of OS, it has the capability to be connected anytime that Windows is online
  - As long as we have Internet access we also have a DirectAccess tunnel.
- We can run both DirectAccess and VPN on the same Windows Server 2016 remote access server.

Summary

- More and more organizations are hiring a work from home workforce
- Need a secure, stable, and efficient way to provide access of corporate data and applications to these mobile workers
- Remote Access role provides two ways for remote access to corporate resources: VPN and DirectAccess
- DirectAccess: a brand new way of looking at remote access: Automatic connectivity