Cisco

Cisco How-to's and configurations

- LACP In Cisco Switch
- Client VPN OS Configuration

LACP In Cisco Switch

Active Mode

To configure a port channel group with LACP and trunking with VLAN 2 as the native VLAN on ports Gigabit Ethernet 45-48, you can follow the steps below:

1. Enter global configuration mode by typing the command:

code

```
configure terminal
```

2. Create a new port channel group by typing the command:

code

```
interface Port-channel 1
```

> *Note:*
>
> *This will create a new port channel interface named Port-channel 1.*

3.Add the range of interfaces GigabitEthernet 2/0/45-48 to the new port channel group and configure it to use LACP mode "active" by typing the command:

code

```
interface range GigabitEthernet 2/0/45-48
channel-group 1``mode active
```

This will add the range of interfaces to the new Port-channel 1 interface and configure it to use LACP mode "active".

Set the LACP system priority and port priority for the new Port-channel interface by typing the command:

code

```
lacp system-priority 65535

lacp port-priority 32768

interface Port-channel 1

lacp mode active
```

This will configure the new Port-channel 1 interface to use LACP mode "active" with a system priority of 65535 and a port priority of 32768.

Set the new Port-channel interface to be a trunk with VLAN 2 as the native VLAN by typing the command:

code

```
interface Port-channel 1
switchport mode trunk
switchport trunk native vlan 2
```

This will configure the new Port-channel 1 interface to be a trunk port with VLAN 2 as the native VLAN.

Save the configuration by typing the command:

code

```
write memory
```

This will save the configuration to the non-volatile memory of the switch, which will ensure that the configuration persists across reboots.

That's it! Your Cisco Catalyst 3650 switch should now have a Port-channel interface named Port-channel 1 with Gigabit Ethernet ports 45-48 configured as a trunk port with VLAN 2 as the native VLAN.

To configure Gigabit Ethernet ports 43-44 on another Port-channel interface with the same configuration as the first Port-channel, you can follow these steps:

Create a new Port-channel interface by typing the command:

code

```
interface Port-channel 2
```

This will create a new Port-channel interface named Port-channel 2.

Add the range of interfaces GigabitEthernet 2/0/43-44 to the new Port-channel interface by typing the command:

code

```
interface range GigabitEthernet 2/0/43-44
channel-group 2
mode active
```

This will add the range of interfaces to the new Port-channel 2 interface and configure it to use LACP mode "active".

Set the LACP system priority and port priority for the new Port-channel 2 interface by typing the command:

code

```
lacp system-priority 65535
lacp port-priority 32768
interface Port-channel 2
lacp mode active
```

This will configure the new Port-channel 2 interface to use LACP mode "active" with a system priority of 65535 and a port priority of 32768.

Set the new Port-channel 2 interface to be a trunk with VLAN 2 as the native VLAN by typing the command:

code

```
interface Port-channel 2
switchport mode trunk
```

```
switchport trunk native vlan 2
```

This will configure the new Port-channel 2 interface to be a trunk port with VLAN 2 as the native VLAN.

Save the configuration by typing the command:

code

```
write memory
```

This will save the configuration to the non-volatile memory of the switch.

To configure Gigabit Ethernet ports 41-42 on another Port-channel interface with the same configuration as the other two Port-channels, you can follow the same steps as above, but use different Port-channel and interface numbers. For example, to create a new Port-channel 3 interface with Gigabit Ethernet ports 41-42, you would use the following commands:

Create a new Port-channel interface by typing the command:

code

```
interface Port-channel 3
```

Add the range of interfaces GigabitEthernet 2/0/41-42 to the new Port-channel interface by typing the command:

code

```
interface range GigabitEthernet 2/0/41-42 channel-group 3 mode active
```

Set the LACP system priority and port priority for the new Port-channel 3 interface by typing the command:

code

```
lacp system-priority 65535 lacp port-priority 32768 interface Port-channel 3
lacp mode active
```

Set the new Port-channel 3 interface to be a trunk with VLAN 2 as the native VLAN by typing the command:

code

```
interface Port-channel 3 switchport mode trunk switchport trunk native vlan 2
```

Save the configuration by typing the command

code

```
write memory
```

This will save the configuration to the non-volatile memory of the switch.

By following these steps, you can create multiple Port-channel interfaces with the same configuration on your Cisco Catalyst 3650 switch.

"Passive Mode"

In Link Aggregation Control Protocol (LACP), there are two modes that can be configured on the switch interface: "active" and "passive".

When a switch interface is configured in "active" mode, it initiates the LACP negotiation process by sending LACP packets to the other end of the link. This means that the interface actively participates in the creation of the link aggregation group.

On the other hand, when a switch interface is configured in "passive" mode, it does not initiate the LACP negotiation process. It simply responds to LACP packets sent by the other end of the link. This means that the interface passively participates in the creation of the link aggregation group.

In general, it is recommended to configure all interfaces in the same link aggregation group with the same LACP mode (either active or passive). If you configure one interface in active mode and another interface in passive mode, there may be a delay in the creation of the link aggregation group, as one interface will be waiting for the other to initiate the LACP negotiation process.

In the example I provided earlier, I configured the physical interfaces to use LACP mode "active" using the command `channel-group 1 mode active`. However, if you want to configure the interfaces to use LACP mode "passive", you can replace "active" with "passive" in the command, like this:

code

```
interface range GigabitEthernet 2/0/41-44 channel-group 1 mode passive
```

This will configure the physical interfaces to use LACP mode "passive" and add them to the Port-channel 1 interface.

LACP IEEE 802.3ad to bundle the four Gigabit Ethernet ports (45-48) together, you will need to create a port channel group and then configure LACP on the port channel interface.

Here are the steps to create a port channel group and enable LACP on the port channel interface:

Enter global configuration mode by typing the command:

code

`configure terminal`

Create a port channel group by typing the command:

code

`interface Port-channel 1`

This will create a new port channel interface named Port-channel 1.

Add the Gigabit Ethernet ports to the port channel group by typing the command:

code

```
interface range GigabitEthernet 45-48
channel-group 1
mode active
```

This will add the four Gigabit Ethernet ports to the Port-channel 1 interface and configure them to use LACP mode "active".

Save the configuration by typing the command:

code

```
write memory
```

This will save the configuration to the non-volatile memory of the switch, which will ensure that the configuration persists across reboots.

That's it! Your Cisco Catalyst 3650 switch should now have a new port channel interface with LACP enabled on Gigabit Ethernet ports 45-48.

To create another port channel group for Gigabit Ethernet ports 43-44 with the same configuration as the existing Port-channel 1, you can use the following steps:

Enter global configuration mode by typing the command:

code

```
configure terminal
```

Create a new port channel group by typing the command:

code

```
interface Port-channel 2
```

This will create a new port channel interface named Port-channel 2.

Add Gigabit Ethernet ports 43-44 to the new port channel group and configure them to use LACP mode "active" by typing the command:

code

```
interface range GigabitEthernet 43-44
channel-group 2
mode active
```

This will add Gigabit Ethernet ports 43-44 to the new Port-channel 2 interface and configure them to use LACP mode "active".

Set the LACP system priority and port priority for the new Port-channel interface to the same values as Port-channel 1 by typing the command:

code

```
lacp system-priority 65535

lacp port-priority 32768

interface Port-channel 2

lacp mode active
```

This will configure the new Port-channel 2 interface to use LACP mode "active" with the same system priority and port priority as the existing Port-channel 1 interface.

Set the new Port-channel interface to be a trunk with VLAN 2 as the native VLAN by typing the command:

code

```
interface Port-channel 2

switchport mode trunk

switchport trunk native vlan 2
```

This will configure the new Port-channel 2 interface to be a trunk port with VLAN 2 as the native VLAN.

Save the configuration by typing the command:

code

```
write memory
```

This will save the configuration to the non-volatile memory of the switch, which will ensure that the configuration persists across reboots.

That's it! Your Cisco Catalyst 3650 switch should now have two Port-channel interfaces: Port-channel 1 with Gigabit Ethernet ports 45-48 and Port-channel 2 with Gigabit Ethernet ports 43-44. Both Port-channel interfaces should have the same LACP configuration and should be configured as trunk ports with VLAN 2 as the native VLAN.

Example Config of a Cisco Catalyst Switch with Link Aggregations:

```
M4P-SW01-5th-CORE#show running-config

Building configuration...

Current configuration : 10325 bytes

!

! Last configuration change at 21:48:30 UTC Thu Mar 16 2023

!

version 16.3

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

!
```

```
hostname M4P-SW01-5th-CORE
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
no aaa new-model
switch 2 provision ws-c3650-48ps
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
license boot level lanbasek9
diagnostic bootup level minimal
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
mode sso
!
!
!
class-map match-any system-cpp-police-topology-control
description Topology control
class-map match-any system-cpp-police-sw-forward
description Sw forwarding, SGT Cache Full, LOGGING
class-map match-any system-cpp-default
description DHCP snooping, show forward and rest of traffic
```

```
class-map match-any system-cpp-police-sys-data

description Learning cache ovfl, Crypto Control, Exception, EGR Exception,
NFL SAMPLED DATA, Gold Pkt, RPF Failed

class-map match-any system-cpp-police-punt-webauth

description Punt Webauth

class-map match-any system-cpp-police-forus

description Forus Address resolution and Forus traffic

class-map match-any system-cpp-police-multicast-end-station

description MCAST END STATION

class-map match-any system-cpp-police-multicast

description Transit Traffic and MCAST Data

class-map match-any system-cpp-police-l2-control

description L2 control

class-map match-any system-cpp-police-dot1x-auth

description DOT1X Auth

class-map match-any system-cpp-police-data

description ICMP_GEN and BROADCAST

class-map match-any system-cpp-police-control-low-priority

description ICMP redirect and general punt

class-map match-any system-cpp-police-wireless-priority1

description Wireless priority 1

class-map match-any system-cpp-police-wireless-priority2

description Wireless priority 2

class-map match-any system-cpp-police-wireless-priority3-4-5

description Wireless priority 3,4 and 5

class-map match-any non-client-nrt-class
```

```
class-map match-any system-cpp-police-routing-control

description Routing control

class-map match-any system-cpp-police-protocol-snooping

description Protocol snooping

!

policy-map port\_child\_policy

class non-client-nrt-class

bandwidth remaining ratio 10

policy-map system-cpp-policy

class system-cpp-police-data

police rate 200 pps

class system-cpp-police-sys-data

police rate 100 pps

class system-cpp-police-sw-forward

police rate 1000 pps

class system-cpp-police-multicast

police rate 500 pps

class system-cpp-police-multicast-end-station

police rate 2000 pps

class system-cpp-police-punt-webauth

class system-cpp-police-l2-control

class system-cpp-police-routing-control

police rate 1800 pps

class system-cpp-police-control-low-priority

class system-cpp-police-wireless-priority1
```

```
class system-cpp-police-wireless-priority2

class system-cpp-police-wireless-priority3-4-5

class system-cpp-police-topology-control

class system-cpp-police-dot1x-auth

class system-cpp-police-protocol-snooping

class system-cpp-police-forus

class system-cpp-default

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Port-channel1

switchport trunk native vlan 5

switchport trunk allowed vlan 2,4,5

switchport mode trunk

lacp max-bundle 4
```

```
!
interface Port-channel2
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
lacp max-bundle 2
!
interface Port-channel3
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
no ip address
negotiation auto
!
interface GigabitEthernet2/0/1
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/2
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/3
switchport access vlan 2
switchport mode access
```

```
!
interface GigabitEthernet2/0/4
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/5
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/6
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/7
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/8
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/9
switchport access vlan 2
switchport mode access
!
```

```
interface GigabitEthernet2/0/10
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/11
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/12
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/13
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/14
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/15
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/16
```

```
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/17
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/18
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/19
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/20
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/21
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/22
switchport access vlan 2
```

```
switchport mode access
!
interface GigabitEthernet2/0/23
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/24
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/25
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/26
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/27
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/28
switchport access vlan 2
switchport mode access
```

```
!
interface GigabitEthernet2/0/29
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/30
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/31
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/32
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/33
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/34
switchport access vlan 2
switchport mode access
!
```

```
interface GigabitEthernet2/0/35
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/36
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet2/0/37
switchport trunk native vlan 5
switchport mode trunk
!
interface GigabitEthernet2/0/38
!
interface GigabitEthernet2/0/39
!
interface GigabitEthernet2/0/40
!
interface GigabitEthernet2/0/41
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet2/0/42
```

```
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet2/0/43
switchport trunk native vlan 5
switchport mode trunk
channel-protocol lacp
channel-group 2 mode active
!
interface GigabitEthernet2/0/44
switchport trunk native vlan 5
switchport mode trunk
channel-protocol lacp
channel-group 2 mode active
!
interface GigabitEthernet2/0/45
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
!
interface GigabitEthernet2/0/46
```

```
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
!
interface GigabitEthernet2/0/47
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
!
interface GigabitEthernet2/0/48
switchport trunk native vlan 5
switchport trunk allowed vlan 2,4,5
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
```

```
!
interface GigabitEthernet2/1/4
!
interface Vlan1
no ip address
!
interface Vlan2
ip address dhcp
!
interface Vlan4
ip address dhcp
!
interface Vlan5
ip address dhcp
!
ip forward-protocol nd
ip http server
ip http secure-server
!
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data
permit tcp any any eq 22
permit tcp any any eq 465
permit tcp any any eq 143
permit tcp any any eq 993
permit tcp any any eq 995
```

```
permit tcp any any eq 1914

permit tcp any any eq ftp

permit tcp any any eq ftp-data

permit tcp any any eq smtp

permit tcp any any eq pop3

ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf

permit udp any any range 16384 32767

permit tcp any any range 50000 59999

ip access-list extended AutoQos-4.0-wlan-Acl-Scavanger

permit tcp any any range 2300 2400

permit udp any any range 2300 2400

permit tcp any any range 6881 6999

permit tcp any any range 28800 29100

permit tcp any any eq 1214

permit udp any any eq 1214

permit tcp any any eq 3689

permit udp any any eq 3689

permit tcp any any eq 11999

ip access-list extended AutoQos-4.0-wlan-Acl-Signaling

permit tcp any any range 2000 2002

permit tcp any any range 5060 5061

permit udp any any range 5060 5061

ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data

permit tcp any any eq 443

permit tcp any any eq 1521
```

```
permit udp any any eq 1521

permit tcp any any eq 1526

permit udp any any eq 1526

permit tcp any any eq 1575

permit udp any any eq 1575

permit tcp any any eq 1630

permit udp any any eq 1630

permit tcp any any eq 1527

permit tcp any any eq 6200

permit tcp any any eq 3389

permit tcp any any eq 5985

permit tcp any any eq 8080

!

!

!

control-plane

service-policy input system-cpp-policy

!

!

vstack

!

line con 0

stopbits 1

line aux 0

stopbits 1
```

```
line vty 0 4
login
line vty 5 15
login
!
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
ap dot11 airtime-fairness policy-name Default 0
ap group default-group
ap hyperlocation ble-beacon 0
ap hyperlocation ble-beacon 1
ap hyperlocation ble-beacon 2
ap hyperlocation ble-beacon 3
ap hyperlocation ble-beacon 4
end
M4P-SW01-5th-CORE#
M4P-SW01-5th-CORE#
```

```
M4P-SW01-5th-CORE#

M4P-SW01-5th-CORE#

M4P-SW01-5th-CORE#
```

Client VPN OS Configuration

This article outlines instructions to configure a client VPN connection on commonly used operating systems.

Learn more with these free online training courses on the Meraki Learning Hub:

- Implementing Remote Access with IPsec Client VPN

Sign in with your Cisco SSO or create a free account to start training.

Android

> **Note**: Android devices running Android 12 and above do not support Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec) VPNs. Devices with existing configurations will continue to work. Client VPN connection cannot be configured on new devices.
>
> To check the Android version of a device, see Check & update your Android version in Google Support.

To configure an Android device to connect to the client VPN, see Connect to a virtual private network (VPN) on Android in Google Support.

The following VPN information is needed to complete the setup:

- **Name**: This can be anything you want to name the connection, for example, "*Work VPN*"
- **Type**: Select **L2TP/IPSEC PSK**
- **Server address**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **IPSec pre-shared key**: Enter the pre-shared key that admin created in **Security & SD-WAN > Configure > Client VPN**

Chrome OS

To configure a Chrome OS device to connect to client VPN, see Set up virtual private networks (VPNs) in Google Support.

The following VPN information is needed to complete the setup:

- **Service name**: This can be anything you want to name this connection, for example, "*Work VPN*"
- **Provider type**: Select **L2TP/IPsec**
- **Server hostname**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **Authentication type**: Select **Pre-shared key**
- **Username**: Credentials for connecting to VPN—if using Meraki authentication, this will be an email address
- **Password**: Credentials for connecting to VPN
- **Pre-shared key**: Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**

iOS

To configure an iOS device to connect to the client VPN, follow these steps:

1. Navigate to **Settings** > **General** > **VPN & Device Management** > **VPN > Add VPN Configuration**
2. **Type**: Set to L2TP
3. **Description**: This can be anything you want to name this connection, for example, "*Work VPN*"
4. **Server**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
   1. Hostname is preferred to improve reliability during WAN failover
   2. This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
5. **Account**: Enter the username
6. **Password**: Enter if desired
   1. If the password is left blank, it will need to be entered each time the device attempts to connect to the client VPN

7. **Secret**: Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**
8. Ensure that **Send All Traffic** is set to on
9. Save the configuration

macOS

> The following authentication methods are supported:
>
> **User authentication:** Active Directory (AD), RADIUS, or Meraki-hosted authentication
> **Machine authentication:** Preshared keys (for example: shared secret)
>
> When using Meraki-hosted authentication, the VPN account and username setting is the user email address entered in the Meraki dashboard.

To configure a macOS device to connect to client VPN, see Set up a VPN connection on Mac in Apple Support.

The following VPN information is needed:

- **Display Name**: This can be anything you want to name this connection, for example, "*Work VPN*"
- **Server Address:** Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **Account Name:** Enter the account name of the user (based on AD, RADIUS, or Meraki cloud authentication)
- **Password:** User password (based on AD, RADIUS or Meraki cloud authentication)
- **Machine Authentication > Shared Secret:** Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**

> Ensure that the MACs network adapter service order includes the VPN interface as the first item (in the list) otherwise all the traffic will not leave on the Client VPN tunnel. For more reference, see Change the order of the network services your Mac uses in Apple support.

Windows

> The following authentication methods are supported:
> User authentication: Active Directory (AD), RADIUS, or Meraki-hosted authentication
> Machine authentication: Pre-shared keys
>
> When using Meraki-hosted authentication, the VPN account and username setting is the user email address entered in the Meraki dashboard.

To configure a **Windows 10 or Windows 11** device to connect to client VPN, see Connect to a VPN in Windows in Microsoft Support page.

The following VPN information is needed to complete the setup:

- In the **Settings app** on your Windows device, select?????? **Network & internet > VPN > Add VPN**.
  - **VPN provider**: Set to Windows (built-in)
  - **Connection name**: This can be anything you want to name this connection, for example, "Work VPN"
  - **Server name or address**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
    - Hostname is preferred to improve reliability during WAN failover
    - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
  - **VPN type**: Select **L2TP/IPsec with pre-shared key**
  - **User name** and **Password**: optional

Windows-build-in-Client-VPN-config.jpg

After the VPN connection has been created, set the Authentication protocols:

1. Choose the VPN connection and then select **Advanced options** > **More VPN properties > Edit > Security Tab**.
   1. **Note:** Alternatively, run **ncpa.cpl** directly from Search or Command prompt to quickly access your VPN adapters.
2. In the **Security** tab, under **Data encryption >** Select **Require encryption (disconnect if sever declines)**
3. Under **Authentication >** Select **Allow these protocols** > Tick the box **Unencrypted password (PAP)**
4. Verify that no other protocols are selected

Windows-build-in-Client-VPN-Security-Tab-Propoerties-config.jpg

>

> Passwords sent over an IPsec tunnel between the client device and the MX are always encrypted, even when using PAP authentication protocols. The password is fully secure and never sent in clear text over the WAN or the LAN.

Linux

To configure a Red Hat Linux device to connect to client VPN, see Configuring a VPN connection in Red Hat Documentation.

To configure an Ubuntu Linux device to connect to client VPN, see Connect to a VPN in Ubuntu Documentation.

The following packages, and their dependencies, are minimum requirements for Linux:

- xl2tpd to implement L2TP
- strongswan or libreswan to implement IPSec

GUI management of the connection requires the network-manager-l2tp-gnome VPN plugin.