

## NCP Line Management

NCP Line Management controls and monitors the data connection between the VPN Client and the central VPN Gateway (tunnel endpoints) It consists of capability characteristics, depending upon one another, that take care of automatically testing VPN connections, disconnecting/reconnecting them and optimizing transmission paths.

Goal settings are correspondingly varied:

- Minimization of connection fees in network selection (ISDN, GPRS/EDGE, UMTS/HSDPA)
- Maintenance of a permanent VPN tunnel for certain applications, e.g. email push service

Capability characteristics in detail:

- Automatic connection establishment
- Channel bundling
- Short-hold mode
- Time out
- Always On Mode
- PDPD (Passive Dead Peer Detection)

### Automatic connection establishment

The connection to the target system (VPN Gateway) can be configured in such a way that it is automatically achieved as soon as there is data to transmit – the VPN Client automatically establishes a tunnel to the VPN Gateway. The way in which the connection is broken can likewise be pre-configured (in the telephone book).

### Channel bundling

By using ISDN as the media type, the NCP Client software bundles up to 8 ISDN B channels into one, as desired, i.e. large amounts of data can be transmitted on up to 8 channels, separately and parallel. This dynamic channel bundling brings about a substantive reduction in transmission times.

### Short-hold mode

Short hold mode serves for cost savings with data connections via time-cycled network choices. Functionality: If no useful data are queued within a certain time period, the connection is automatically physically broken, while they continue to exist logically between applications (server-teleworker spaces). The user does not have to – depending on the configuration – completely log on again, i.e. he can, when new data are available for transmission and the physical connection is automatically achieved, work again directly.

Short hold mode also results in optimal usage for the tunnel of a VPN gateway, i.e. it is not unnecessarily blocked by teleworkers.

### Time out

With the parameter time out, the time frame is determined that must elapse after the last data movement (either received or sent) before a reconnection automatically follows. The time out runs in the background and counts backward, e.g. 60 seconds. If the data transfers follows in this time, the connection to the VPN gateway is automatically physically and logically broken.

### Always on mode for Windows Mobile (WinCE)

The purpose of "Always on Mode" for Windows Mobile (WinCE) is the permanent maintenance of a VPN tunnel between VPN Client and VPN Gateway. The teleworker must remain constantly online, e.g. due to email push service. Therefore, every 20 seconds the client exchanges data packets with the VPN Gateway. These lead to costs in public transmission networks. For this reason, this performance feature is preferably found in the LAN/WLAN application.

### PDPD for Windows Mobile (WinCE)

PDPD (Passive Dead Peer Detection) is a variant of DPD (Dead Peer Detection, RFC3706). The sense of DPD is to prepare a mechanism to indicate whether a VPN connection or VPN tunnel is still established. For this, it is required that control data (DPD packets) be transmitted in certain time intervals (see above). This has two impacts, above all with "Ultra Mobile Devices" (PDA, Smartphones):

1. It accrues transmission costs
2. With Windows CE terminals, it leads to supplemental load on the batteries, since the send/receive module must be activated continuously

Likewise, PDPD monitors the existence of a VPN tunnel, to be sure *without* sending data packets.

No costs accrue and it doesn't lead to the intensified battery load of a CE device.

If it is determined that no tunnel is established, e.g. in a dead zone, a specified routine for its reconnection is initiated:

- Manually (via API, command line)
- Automatically (automatic connection establishment, short hold mode)