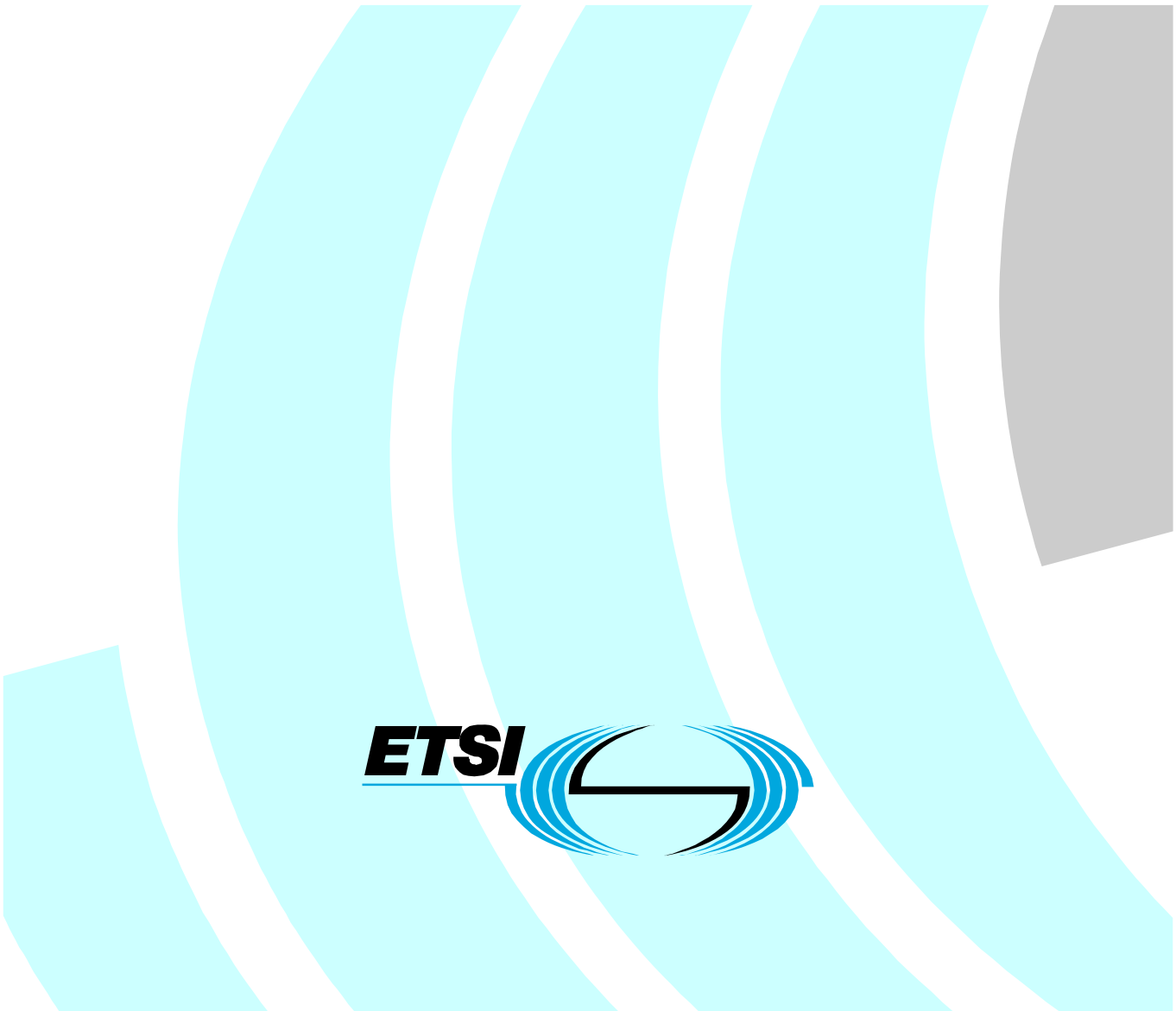
ETSI TR 102 607 V1.1.1 (2007-10)

Technical Report

**Speech Processing, Transmission and Quality Aspects (STQ);
TCP IP Stack Parameter Settings for
Microsoft Windows XP and Microsoft Windows Vista;
Comparison and Recommendations**



Reference
DTR/STQ-000114m

Keywords
configuration, transport

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Speech Processing, Transmission and Quality Aspects (STQ).

1 Scope

The present document points out some differences between the TCP IP Stack implementations included in the Microsoft Windows XP and Microsoft Windows Vista operating systems by providing an overview of default settings currently used. It gives recommendations on the topic of TCP IP Stack configuration parameter tuning with respect to end-to-end quality of service measurements to be performed in digital wireless networks.

Furthermore, the present document provides an overview of TCP IP parameter configuration changes as commonly applied by software provided for the respective operating system by network operators in order for the end-user to access the operators network.

If not explicitly stated differently, the English versions of Microsoft Windows XP (including Service Pack 2) and Microsoft Windows Vista operation systems shall be taken as reference operating systems for the information provided in the present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Informative references

[1] Microsoft TechNet: http://support.microsoft.com/kb/120642.

[2] Microsoft white paper: "TCP/IP Registry Values for Microsoft Windows Vista and Windows Server 'Longhorn'".

[3] Microsoft TechNet: http://technet2.microsoft.com/windowsserver/en/library/db56b4d4-a351-40d5-b6b1-998e9f6f41c91033.mspx?mfr=true.

[4] ETSI TS 102 250-5 (V1.3.1): "Speech Processing, Transmission and Quality Aspects (STQ); QoS aspects for popular services in GSM and 3G networks; Part 5: Definition of typical measurement profiles".

[5] ETSI TS 102 250 (all parts): "Speech Processing, Transmission and Quality Aspects (STQ); QoS aspects for popular services in GSM and 3G networks".

[6] IETF RFC 1323: "TCP Extensions for High Performance".

[7] IETF RFC 793: "Transmission Control Protocol".

[8] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[9] IETF RFC 1256: "ICMP Router Discovery Messages".

[10] IETF RFC 2018: "TCP Selective Acknowledgment Options".

[11] IETF RFC 3481: "TCP over Second (2.5G) and Third (3G) Generation Wireless Networks".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APIPA	Automatic Private IP Addressing
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuation Protocol
DIX	Digital, Intel, Xerox
DNS	Domain Name System
GPRS	General Packet Radio Services
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LAN	Local Area Network
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NLBS	Network Load Balancing Service
RFC	Request For Comments
RTT	Round-Trip Time
SACK	Selective ACKnowledgment
SNAP	Sub Network Access Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
VPN	Virtual Private Network

4 TCP IP Parameter Overview

This clause lists all relevant parameters in an overview table, followed by a detailed explanation for each parameter, grouped in three sections:

- Parameters found in both Windows XP and Vista.
- Parameters found in Windows Vista only.
- Parameters found in Windows XP only.

NOTE: Windows XP uses the same TCP IP Stack implementation as Windows Server 2003, while Windows Vista uses the same TCP IP Stack implementation as the upcoming Windows Server 2007/2008 (formerly Windows Server Longhorn).

4.1 Overview Table

Table 1: Overview of TCP parameters described in the present document

Parameter name	Available:		Optional:	
	XP	Vista	XP	Vista
ArpAlwaysSourceRoute	X		X	
ArpRetryCount		X		
ArpUseEtherSNAP	X	X	X	
DatabasePath	X			
DefaultGateway	X	X		
DefaultTTL	X	X	X	
DisabledComponents		X		
DisableDHCPMediaSense		X		
DisableIPSourceRouting		X		
DisableTaskOffload		X		
Domain	X			
EnableAddrMaskReply		X		
EnableBcastArpReply		X		
EnableDeadGWDetect	X		X	
EnableDhcp	X			
EnableICMPRedirect		X		
EnableMulticastForwarding		X		
EnablePMTUBHDetect	X	X	X	
EnablePMTUDiscovery	X	X	X	
ForwardBroadcasts	X			
ForwardBufferMemory	X		X	
GlobalMaxWindowSize	X		X	
Hostname	X			
IGMPLevel	X	X	X	
IGMPVersion		X		
InterfaceMetric		X		
IPAddress	X	X		
IPAutoconfigurationAddress		X		
IPAutoconfigurationEnabled		X		
IPAutoconfigurationMask		X		
IPAutoconfigurationSubnet		X		
IPEnableRouter	X	X		
KeepAliveInterval	X	X	X	
KeepAliveTime	X	X	X	
MTU	X	X	X	
NameServer	X			
NumForwardPackets	X		X	
PerformRouterDiscovery		X		
SackOpts	X		X	
SearchList	X			
SolicitationAddressBcast		X		
SubnetMask	X	X		
Tcp1323Opts	X	X	X	
TcpAckFrequency		X		
TcpDelAckTicks	X	X	X	
TcpInitialRTT	X		X	
TcpFinWait2Delay		X		
TcpMaxConnectRetransmissions	X		X	
TcpMaxDataRetransmissions	X	X	X	
TcpMaxDupAcks	X	X	X	
TcpNumConnections	X		X	
TcpTimedWaitDelay	X	X	X	
TcpUseRFC1122UrgentPointer	X	X	X	
TcpWindowSize	X		X	
TypeOfInterface		X		
UseZeroBroadcast	X	X		

4.2 Parameters found in Windows Vista and XP

NOTE 1: Descriptions are taken from Microsoft TechNet, see reference [1].

ArpUseEtherSNAP *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False or True)
Default: 0 (False)
Description: Setting this parameter to 1 will force TCP/IP to transmit Ethernet packets using 802.3 SNAP encoding. By default, the stack transmits packets in DIX Ethernet format. It will always receive both formats.

DefaultGateway

Key (XP): Tcpip\Parameters\Interfaces*ID for Adapter*
Key (Vista) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_MULTI_SZ - List of dotted decimal IP addresses
Valid Range: Any set of valid IP addresses
Default: None
Description: This parameter specifies the list of gateways to be used to route packets not destined for a subnet that the computer is directly connected to, and for which a more specific route does not exist. This parameter, if it has a valid value, overrides the DhcpDefaultGateway parameter.

DefaultTTL *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Number of seconds/hops
Valid Range: 1-255
Default: 32 for Windows NT version 3.51
Default: 128 for Windows NT version 4.0
Description: Specifies the default Time To Live (TTL) value set in the header of outgoing IP packets. The TTL determines the maximum amount of time an IP packet may live in the network without reaching its destination. It is effectively a limit on the number of routers an IP packet may pass through before being discarded.

EnablePMTUBHDetect *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False, True)
Default: 0 (False)
Description: Setting this parameter to 1 (True) causes TCP to try to detect "Black Hole" routers while doing Path MTU Discovery. A "Black Hole" router does not return ICMP Destination Unreachable messages when it needs to fragment an IP datagram with the Don't Fragment bit set. TCP depends on receiving these messages to perform Path MTU Discovery. With this feature enabled, TCP will try to send segments without the Don't Fragment bit set if several retransmissions of a segment go unacknowledged. If the segment is acknowledged as a result, the MSS will be decreased and the Don't Fragment bit will be set in future packets on the connection. Enabling black hole detection increases the maximum number of retransmissions performed for a given segment.

EnablePMTUDiscovery *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False, True)
Default: 1 (True)
Description: Setting this parameter to 1 (True) causes TCP to attempt to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to machines on the local subnet.

IGMPLevel *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Number
Valid Range: 0,1,2
Default: 2
Description: This parameter determines to what extent the system supports IP multicasting and participates in the Internet Group Management Protocol. At level 0, the system provides no multicast support. At level 1, the system may only send IP multicast packets. At level 2, the system may send IP multicast packets and fully participate in IGMP to receive multicast packets.

IPAddress

Key (XP): Tcpip\Parameters\Interfaces*ID for Adapter*
Key (Vista) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_MULTI_SZ - List of dotted- decimal IP addresses
Valid Range: Any set of valid IP addresses
Default: None
Description: This parameter specifies the IP addresses of the IP interfaces to be bound to the adapter. If the first address in the list is 0.0.0.0, then the primary interface on the adapter will be configured from DHCP. A system with more than one IP interface for an adapter is called "logically multihomed". There must be a valid subnet mask value in the SubnetMask parameter for each IP address specified in this parameter.

IPEnableRouter

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0 or 1 (False or True)
Default: 0 (False)
Description: Setting this parameter to 1 (True) causes the system to route IP packets between the networks that it is connected to.

KeepAliveInterval *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Time in milliseconds
Valid Range: 1 - 0xFFFFFFFF
Default: 1 000 (one second)
Description: This parameter determines the interval separating keep alive retransmissions until a response is received. Once a response is receive, the delay until the next keep alive transmission is again controlled by the value of KeepAliveTime. The connection will be aborted after the number of retransmissions specified by TcpMaxDataRetransmissions have gone unanswered.

KeepAliveTime *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Time in milliseconds
Valid Range: 1 - 0xFFFFFFFF
Default: 7 200 000 (two hours)
Description: The parameter controls how often TCP attempts to verify that an idle connection is still intact by sending a keep alive packet. If the remote system is still reachable and functioning, it will acknowledge the keep alive transmission. Keep alive packets are not sent by default. This feature may be enabled on a connection by an application.

MTU *(Optional in Windows XP)*

Key (XP): Tcpip\Parameters\Interfaces*ID for Adapter*
Key (Vista) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_DWORD Number
Valid Range: 68 - *the MTU of the underlying network*
Default: 0xFFFFFFFF
Description: This parameter overrides the default Maximum Transmission Unit (MTU) for a network interface. The MTU is the maximum packet size in bytes that the transport will transmit over the underlying network. The size includes the transport header. Note that an IP datagram may span multiple packets. Values larger than the default for the underlying network will result in the transport using the network default MTU. Values smaller than 68 will result in the transport using an MTU of 68.

SubnetMask

Key (XP): Tcpip\Parameters\Interfaces*ID for Adapter*
Key (Vista) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_MULTI_SZ - List of dotted decimal IP addresses
Valid Range: Any set of valid IP addresses.
Default: None
Description: This parameter specifies the subnet masks to be used with the IP interfaces bound to the adapter. If the first mask in the list is 0.0.0.0, then the primary interface on the adapter will be configured via DHCP. There must be a valid subnet mask value in the this parameter for each IP address specified in the IPAddress parameter.

Tcp1323Opts (Optional in Windows XP)

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD—number (flags)
Valid Range: 0 or 2
0 (disable the use of the TCP timestamps option)
2 (enable the use of the TCP timestamps option)
Default: No value.
Description: This value controls the use of the RFC 1323 [6] TCP Timestamp option. The default behaviour of the TCP/IP stack is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

NOTE 2: Additional information on the valid Range (see reference [3]):

The valid range is 0, 1, 2, 3, with:

- 0 (disable RFC 1323 [6] options);
- 1 (window scaling enabled only);
- 2 (timestamps enabled only);
- 3 (both options enabled).

NOTE 3: Vista probably without Scaling options (for further study).

NOTE 4: Additional information on the default value (see reference [3]):

The default behaviour is as follows: do not use the Timestamp and Window Scale options when initiating TCP connections but use them if the TCP peer that is initiating communication includes them in the SYN segment.

Description *(see reference [3]): This parameter controls the use of RFC 1323 [6] Timestamp and Window Scale TCP options. Explicit settings for timestamps and window scaling are manipulated with flag bits. Bit 0 controls window scaling, and bit 1 controls timestamps.*

TcpDelAckTicks (Optional in Windows XP)

Key (Vista/XP) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_DWORD—number
Valid Range: 2–6
Default: 2
Description: Specifies the number of 100 millisecond intervals to use for the delayed-ACK timer on a per-interface basis. By default, the delayed-ACK timer is 200 milliseconds. If you set this value to 0 or 1, the delayed-ACK time is 200 milliseconds. Microsoft does not recommend changing this value from the default without careful study of the environment.

***For further study**: Setting this value to 0 in Microsoft Windows XP used to disable delayed acknowledgments, causing the computer to immediately ACK every packet it receives.*

TcpMaxDataRetransmissions *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Default: 5
Description: This parameter controls the number of times TCP will retransmit an individual data segment (non connect segment) before aborting the connection. The retransmission timeout is doubled with each successive retransmission on a connection. It is reset when responses resume. The base timeout value is dynamically determined by the measured round-trip time on the connection.

TcpMaxDupAcks *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Number
Valid Range: 1-3
Default: 2
Description: Specifies how many duplicate ACKs (ACKs for the same sequence numbers) constitute a signal to retransmit a segment. If you set the value of this entry to 1, then the system retransmits a segment when it receives an ACK for a segment with a sequence number that is less than the number of the segment currently being sent.

When data arrives with a sequence number that is greater than expected, the receiver assumes that data with the expected number was dropped, and it immediately sends an ACK with the ACK number set to the expected sequence number. The receiver sends ACKs set to the same missing number each time it receives a TCP segment that has a sequence number greater than expected. The sender recognizes the duplicate ACKs and sends the missing segment.

TcpTimedWaitDelay *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Time in seconds
Valid Range: 30-300 (decimal)
Default: 0xF0 (240 decimal)
Description: This parameter determines the length of time that a connection will stay in the TIME_WAIT state when being closed. While a connection is in the TIME_WAIT state, the socket pair cannot be re- used. This is also known as the "2MSL" state, as by RFC the value should be twice the maximum segment lifetime on the network.
See RFC 793 [7] for further details.

TcpUseRFC1122UrgentPointer *(Optional in Windows XP)*

Key (Vista/XP): Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False, True)
Default: 0 (False)
Description: This parameter determines whether TCP uses the RFC 1122 [8] specification for urgent data or the mode used by BSD- derived systems. The two mechanisms interpret the urgent pointer in the TCP header and the length of the urgent data differently. They are not interoperable. Windows NT defaults to BSD mode.

NOTE 5: Windows XP defaults to BSD mode.

UseZeroBroadcast

Key (XP): Tcpip\Parameters\Interfaces*ID for Adapter*
Key (Vista) : Tcpip\Parameters\Interfaces*InterfaceGUID*
Value Type: REG_DWORD - Boolean
Valid Range: 0 or 1 (False or True)
Default: 0 (False)
Description: If this parameter is set to 1 (True), then IP will use zeros- broadcasts (0.0.0.0) instead of ones-broadcasts (255.255.255.255). Most systems use ones- broadcasts, but some systems derived from BSD implementations use zeros-broadcasts. Systems that use different broadcasts will not interoperate well on the same network.

4.3 Parameters found in Windows Vista only

NOTE: Descriptions taken from Microsoft white paper, see reference [2].

ArpRetryCount

Key: Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 0–3
Default: 3
Description: This value controls the number of times that the computer sends a gratuitous Address Resolution Protocol (ARP) Request message for its own IPv4 address(es) while initializing. Gratuitous ARP requests are sent to ensure that the IPv4 address is not already in use on the locally attached subnet. The value controls the actual number of ARP requests sent, not the number of retries.

DisabledComponents

Key: Tcpip6\Parameters
Value Type: REG_DWORD
Valid Range: 0-FF
Default: 0
Description: This value can be used to modify IPv6 capabilities. The DisabledComponents registry value is a bit mask that controls the following series of flags, starting with the low order bit (Bit 0):

- Bit 0 Set to 1 to disable all IPv6 tunnel interfaces, including the Intra-site Automatic Tunnel Addressing Protocol (ISATAP), 6to4, and Teredo tunnel interfaces. Default value is 0. For more information about ISATAP, 6to4, and Teredo, see IPv6 Transition Technologies at: http://www.microsoft.com/technet/network/ipv6/ipv6coexist.mspx.
- Bit 1 Set to 1 to disable all 6to4-based interfaces. Default value is 0.
- Bit 2 Set to 1 to disable all ISATAP-based interfaces. Default value is 0.
- Bit 3 Set to 1 to disable all Teredo-based interfaces. Default value is 0.
- Bit 4 Set to 1 to disable IPv6 over all non-tunnel interfaces, including LAN interfaces and Point-to-Point Protocol (PPP)-based interfaces. Default value is 0.
- Bit 5 Set to 1 to modify the default prefix policy table to prefer IPv4 to IPv6 when attempting connections. Default value is 0.

You must restart the computer for the changes to the DisabledComponents registry value to take effect.

DisableDHCPMediaSense

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: This value can be used to control DHCP Media Sense behaviour. If set to 1, the DHCP client ignores Media Sense events from the interface. By default, Media Sense events trigger the DHCP client to take an action, such as attempting to obtain a lease when a connect event occurs, or invalidating the interface and routes when a disconnect event occurs.

DisableIPSourceRouting

Key: Tcpip\Parameters, Tcpip6\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1, 2

- 0 - forward all packets;
- 1 - do not forward source routed packets;
- 2 - drop all incoming source routed packets.

Default: 1 for IPv4 and 0 for IPv6
Description: IP source routing is a mechanism that allows the sender to determine the IP route that a packet should take through the network. The Ping and Tracert tools have command-line options to specify source routing.

DisableMediaSenseEventLog

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: This value can be used to disable logging of DHCP Media Sense events. By default, Media Sense events (connection/disconnection from the network) are logged in the event log for troubleshooting purposes.

DisableTaskOffload

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: This value instructs the TCP/IP stack to disable offloading of tasks to the network adapter for troubleshooting and testing purposes.

EnableAddrMaskReply

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: This value controls whether the computer responds to an Internet Control Message Protocol (ICMP) address mask request.

EnableBcastArpReply

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 1 (true)
Description: This value controls whether the computer responds to an ARP request when the source Ethernet address in the ARP request is not unicast. Network Load Balancing Service (NLBS) will not work properly if this value is set to 0.

EnableICMPRedirect

Key: Tcpip\Parameters
Value Type: REG_DWORD--BOOLEAN
Valid Range: 0, 1 (False, True)
Default: 1 (True)
Recommendation: 0 (False)
Description: This value controls whether the TCP/IP stack will update its IPv4 routing table in response to ICMP Redirect messages that are sent to it by network devices such as a routers.

EnableMulticastForwarding

Key: Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: The routing service uses this value to control whether or not IP multicasts are forwarded. This value is created by the Routing and Remote Access service.

IGMPVersion

Key: Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 2, 3, 4
Default: 4
Description: This value specifies the version of IGMP to use. Specify 2 for IGMP version 1, 3 for IGMP version 2 or 4 for IGMP version 3.

InterfaceMetric

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD—number
Valid Range: 1-9999
Description: This value specifies a fixed interface metric for an interface.

IPAutoconfigurationAddress

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_SZ—String
Valid Range: A valid IPv4 address
Default: None
Description: This value stores the APIPA autoconfiguration IPv4 address chosen by the DHCP client. This value should not be altered.

IPAutoconfigurationEnabled

Key: Tcpip\Parameters, Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (false, true)
Default: 1 (true)
Description: This value enables or disables IPv4 autoconfiguration using APIPA. This value can be set globally or per interface. If a per-interface value is present, it overrides the global value for that interface.

IPAutoconfigurationMask

Key: Tcpip\Parameters, Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_SZ—String
Valid Range: A valid IP subnet mask
Default: 255.255.0.0
Description: This value controls the subnet mask assigned to the client using Automatic Private IP Addressing (APIPA) autoconfiguration. This value can be set globally or per interface. If a per-interface value is present, it overrides the global value for that interface.

IPAutoconfigurationSubnet

Key: Tcpip\Parameters, Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_SZ—String
Valid Range: A valid IP subnet
Default: 169.254.0.0
Description: This value controls the initial address prefix used by APIPA autoconfiguration when selecting an IPv4 address for the client. This value can be set globally or per interface. If a per-interface value is present, it overrides the global value for that interface.

PerformRouterDiscovery

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD
Valid Range: 0, 1, 2

- 0 (disabled);
- 1 (enabled);
- 2 (enable only if DHCP sends the Perform Router Discovery option).

Default: 2, DHCP-controlled but off by default.
Description: This value controls whether the TCP/IP stack attempts to perform IPv4 router discovery (RFC 1256 [9]) on a per-interface basis. See also SolicitationAddressBcast.

SolicitationAddressBcast

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD
Valid Range: 0, 1 (false, true)
Default: 0 (false)
Description: This value controls whether the TCP/IP stack will send IPv4 router discovery messages as broadcasts instead of multicasts (RFC 1256 [9]). By default, if IPv4 router discovery is enabled, router discovery solicitations are sent to the all-routers multicast group (224.0.0.2). See also PerformRouterDiscovery.

TcpAckFrequency

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD—number
Valid Range: 0–255
Default: 2
Description: Specifies the number of TCP acknowledgements (ACKs) that will be outstanding before the delayed ACK timer is ignored. Microsoft does not recommend changing this value from the default without careful study of the environment.

TcpFinWait2Delay

Key: Tcpip\Parameters
Value Type: REG_DWORD—number
Valid Range: 30–294 967 295
Default: 120
Description: This value controls the maximum number of seconds that a TCP connection will remain in the FIN_WAIT_2 state. For more information, see RFC 793 [7].

TypeOfInterface

Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD
Valid Range: 0, 1, 2, 3
Default: 0 (allow multicast and unicast)
Description: This value determines whether the interface gets routes plumbed for unicast, multicast, or both traffic types, and whether those traffic types can be forwarded. If it is set to 0, both unicast and multicast traffic are allowed. If it is set to 1, unicast traffic is disabled. If it is set to 2, multicast traffic is disabled. If it set to 3, both unicast and multicast traffic are disabled. Since this value affects forwarding and routes, it may still be possible for a local application to send multicasts out over an interface, if there are no other interfaces in the computer that are enabled for multicast, and a default route exists.

4.4 Parameters found in Windows XP only

NOTE 1: Descriptions taken from Microsoft TechNet, see reference [1] and [3].

ArpAlwaysSourceRoute *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False or True)
Default: 0 (False)
Description: Setting this parameter to 1 will force TCP/IP to transmit ARP queries with source routing enabled on Token Ring networks. By default, the stack transmits ARP queries without source routing first and retries with source routing enabled if no reply was received.

DatabasePath

Key: Tcpip\Parameters
Value Type: REG_EXPAND_SZ - Character string
Valid Range: A valid Windows NT file path
Default: %SystemRoot%\system32\drivers\etc
Description: This parameter specifies the path to the standard internet database files (HOSTS, LMHOSTS, NETWORKS, PROTOCOLS). It is used by the Windows Sockets interface.

Domain

Key: Tcpip\Parameters
Value Type: REG_SZ - Character string
Valid Range: Any valid DNS domain name
Default: None
Description: This parameter specifies the DNS domain name of the system. It is used by the Windows Sockets interface.

EnableDeadGWDetect *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0,1 (False, True)
Default: 1 (True)
Description: Setting this parameter to 1 causes TCP to perform Dead Gateway Detection. With this feature enabled, TCP will ask IP to change to a backup gateway if it retransmits a segment several times without receiving a response. Backup gateways may be defined in the Advanced section of the TCP/IP configuration dialog in the Network Control Panel.

EnableDhcp

Key: Tcpip\Parameters\Interfaces\ID for Adapter
Value Type: REG_DWORD - Boolean
Valid Range: 0 or 1 (False or True)
Default: 0 (False) Description: If this parameter is set to 1 (True), then the DHCP client service will attempt to configure the first IP interface on the adapter using DHCP.

ForwardBroadcasts

Key: Tcpip\Parameters
Value Type: REG_DWORD - Boolean
Valid Range: 0 or 1 (False or True)
Default: 0 (False)
Description: Forwarding of broadcasts is not supported. This parameter is ignored.

ForwardBufferMemory *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Number of bytes
Valid Range: network MTU - some reasonable
value smaller than 0xFFFFFFFF
Default: 74 240 (enough for fifty 1 480-byte
packets, rounded to a multiple of 256)
Description: This parameter determines how much memory IP allocates to store packet data in the router packet queue. When this buffer space is filled, the router begins discarding packets at random from its queue. Packet queue data buffers are 256 bytes in length, so the value of this parameter should be a multiple of 256. Multiple buffers are chained together for larger packets. The IP header for a packet is stored separately. This parameter is ignored and no buffers are allocated if the IP router is not enabled.

GlobalMaxTcpWindowSize *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD-Number of bytes
Valid Range: 0-0x3FFFFFFF (1073741823 decimal; however, values greater than 64 KB can only be achieved when connecting to other systems that support RFC 1323 [6] window scaling, which is discussed in the TCP section of the present document.)
Default: This parameter does not exist by default.
Description: The TcpWindowSize parameter can be used to set the receive window on a per-interface basis. This parameter can be used to set a global limit for the TCP window size on a system-wide basis.

Hostname

Key: Tcpip\Parameters
Value Type: REG_SZ - Character string
Valid Range: Any valid DNS hostname
Default: The computername of the system
Description: This parameter specifies the DNS hostname of the system, that will be returned by the "hostname" command.

NameServer

Key: Tcpip\Parameters
Value Type: REG_SZ - A space delimited list of dotted decimal IP addresses
Valid Range: Any set of valid IP address
Default: None (Blank)
Description: This parameter specifies the DNS name servers to be queried by Windows Sockets to resolve names.

NumForwardPackets *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD Number
Valid Range: 1 - some reasonable value
smaller than 0xFFFFFFFF Default: 50
Description: This parameter determines the number of IP packet headers allocated for the router packet queue. When all headers are in use, the router will begin to discard packets at random from the queue. This value should be at least as large as the ForwardBufferMemory value divided by the maximum IP data size of the networks connected to the router. It should be no larger than the ForwardBufferMemory value divided by 256, since at least 256 bytes of forward buffer memory are used for each packet. The optimal number of forward packets for a given ForwardBufferMemory size depends on the type of traffic carried on the network and will be somewhere in between these two values. This parameter is ignored and no headers are allocated if the router is not enabled.

SackOpts *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD-Boolean
Valid Range: 0, 1 (false, true)
Default: 1 (true)
Description: This parameter controls whether or not Selective Acknowledgment (SACK) support, as specified in RFC 2018 [10], is enabled.

SearchList

Key: Tcpip\Parameters
Value Type: REG_SZ - Delimited list of DNS domain name suffixes
Valid Range: Any set of valid DNS domain name suffixes
Default: None
Description: This parameter specifies a list of domain name suffixes to append to a name to be resolved via the DNS if resolution of the unadorned name fails. By default, the value of the Domain parameter is appended only. This parameter is used by the Windows Sockets interface.

TcpInitialRTT *(Optional)*

PARAMETER: TcpInitialRTT
Key: Tcpip\Parameters\Interfaces\interfaceGUID
Value Type: REG_DWORD-number
Valid Range: 0-0xFFFF
Default: 3
Description: This parameter controls the initial time-out used for a TCP connection request and initial data retransmission on a per-interface basis. Use caution when tuning with this parameter because exponential back off is used. Setting this value to larger than 3 results in much longer time-outs to nonexistent addresses.

TcpMaxConnectRetransmissions *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Default: 3 (in Windows NT)
Default: 2 (in Windows 2000)
Description: This parameter determines the number of times TCP will retransmit a connect request (SYN) before aborting the attempt. The retransmission timeout is doubled with each successive retransmission in a given connect attempt. The initial timeout value is three seconds.

TcpNumConnections *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Number
Valid Range: 0 - 0xfffffe
Default: 0xfffffe
Description: This parameter limits the maximum number of connections that TCP may have open simultaneously.

TcpWindowSize *(Optional)*

Key: Tcpip\Parameters
Value Type: REG_DWORD - Number of bytes
Valid Range: 0 - 0xFFFF
Default: The smaller of 0xFFFF; or
(The larger of four times the maximum TCP data size on the network; or
8 192 rounded up to an even multiple of the network TCP data size.)
The default is 8 760 for Ethernet.
Description: This parameter determines the maximum TCP receive window size offered by the system. The receive window specifies the number of bytes a sender may transmit without receiving an acknowledgment. In general, larger receive windows will improve performance over high (delay * bandwidth) networks. For highest efficiency, the receive window should be an even multiple of the TCP Maximum Segment Size (MSS).

NOTE 2: Additional information on the default value:

The smaller of the following values will be used:

- 0xFFFF.
- GlobalMaxTcpWindowSize (another registry parameter).
- The larger of four times the MSS.
- 16 384 rounded up to an even multiple of the MSS.
- The stack also tunes itself based on the media speed:
  - Below 1 Mbps: 8 KB.
  - 1 Mbps - 100 Mbps: 17 KB.
  - Greater than 100 Mbps: 64 KB.

NOTE 3: The default can start at 17 520 for Ethernet, but may shrink slightly when the connection is established to another computer that supports extended TCP header options, such as Selective Acknowledgements (SACK) and TCP Timestamps, because these options increase the size of the TCP header beyond the usual 20 bytes, leaving slightly less room for data.

NOTE 4: This parameter is both a per-interface parameter and a global parameter, depending on where the registry key is located. If there is a value for a specific interface, that value overrides the systemwide value. See also GobalMaxTcpWindowSize.

5 Default TCP IP Stack Settings of Microsoft Operating Systems

5.1 Default TCP IP Stack Settings of the Windows XP Operating System

The following TCP/IP Parameter Settings are common Windows XP default settings.

Global TCP/IP Parameter Settings:

Key Name: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Parameter Name	Value
NV Hostname	MY-MACHINE (see note)
DataBasePath	%SystemRoot%\System32\drivers\etc
NameServer	
ForwardBroadcasts	0
IPEnableRouter	0
Domain	
Hostname	MY-MACHINE (see note)
SearchList	
UseDomainNameDevolution	1
EnableICMPRedirect	1
DeadGWDetectDefault	1
DontAddDefaultGatewayDefault	0
EnableSecurityFilters	0
NOTE: The provided value is just an examples and may vary.	

Common Adapter Parameter Settings:

Key Name: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{ }

Parameter Name	Value
UseZeroBroadcast	0
EnableDHCP	0
IPAddress	127.0.0.1 (see note)
SubnetMask	127.0.0.1 (see note)
DefaultGateway	
EnableDeadGWDetect	1
DontAddDefaultGateway	0
NOTE: The provided value is just an examples and may vary.	

Winsock Parameter Settings:

Key Name: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Winsock

Parameter Name	Value
UseDelayedAcceptance	0
HelperDllName	%SystemRoot%\System32\wshtcpip.dll
MaxSockAddrLength	16
MinSockAddrLength	16

5.2 Default TCP IP Stack Settings of the Windows Vista Operating System

For further study: Default TCP/IP Parameter Settings for Windows Vista.

6 General Recommendations

NOTE 1: The IETF (Internet Engineering Task Force) has formed an own work group called "Performance Implications of Link Characteristics". PILC develops recommendations for optimizing and modifying IETF-protocols (e.g. TCP) in network environments with problematic transmission capabilities.

NOTE 2: Most of the proposed recommendation are given with respect to 2G networks.

For further study: Alignment with recommendations for other digital wireless networks than 2G.

6.1 Recommendations for Single Parameters

EnablePMTUBHDetect *(Vista / XP optional)*

Recommendations: If Path MTU Discovery is going to be used, this option should be enabled (set to 1) to ensure the functionality of Path MTU Discovery.

NOTE 1: Windows XP SP2 and Windows Vista enables black hole detection by default, and changes the MTU to 536 bytes if retransmissions occurs.

EnablePMTUDiscovery *(Vista / XP optional)*

Recommendations: This parameter should stay at default value 1, if the MTU is not known for the network to be used. Furthermore, a smart VPN Client checking for the possible MSS on the network connection to be used could also use the outcome of Path MTU Discovery. Together with the knowledge about the extra data needed for encryption information, the VPN client would then be able set the MTU of the encrypted TCP sockets to a reasonable size. Thus, Path MTU Discovery could be enabled in such a scenario as well. Other than that, Path MTU Discovery should be disabled.

ForwardBufferMemory *(XP only, optional)*

Recommendations: This value should stay at default value 74 240. For the setting to take effect, the option IPEnableRouter must be enabled (can be done using the network tool in the control panel or by editing the registry).

GlobalMaxTcpWindowSize (XP only, optional)

Recommendation: This parameter should only be used, if it is intended to change the global limit. It has been listed here since it has an impact on the default value of TcpWindowSize parameter described below.

KeepAliveTime *(Vista / XP optional)*

Recommendations: This parameter should be set to equal the value of the PDP context timeout. This timeout can be found out from the network operator. In German networks, this timeout is usually set to 15 minutes. Here, for applications that need an open socket, this parameter should be set to 900 000 (15 minutes), which in hexadecimal format is DBBA0. Please note that since all IP traffic after context activation is billed, the keep alive packets will of course be billed as well.

MTU *(Vista / XP optional)*

Recommendations: Evaluations in German networks have shown that 1 448 is a reliable value, if the network operator uses Ericsson or Siemens hardware. On the other hand, if the network operator uses Nokia hardware where a MSS of 1 380 is the default, a value of 1 420 should be used for the MTU parameter. Even smaller values must be chosen, if it is known beforehand that for example a VPN tunnel is going to be used and thus the packets need to be smaller to avoid fragmentation. Especially in this scenario, it is very important to choose an appropriate MTU. Here, the reassembling of fragmentized data packets is a well known problem. Other than that, the proposed value should be used even if it is known that mostly interactive traffic will occur on the connection. Instead of lowering MTU size, the push flag should be set from the application level, if urgent data needs to be sent.

NumForwardPackets *(XP only, optional)*

Recommendations: If the computer is used as a router, e.g. between LAN and GPRS, it is advised to enter a reasonable value.

NOTE 2: This setting takes only effect, if the option IPEnableRouter is enabled (can be done using the network tool in the control panel or by editing the registry).

EXAMPLE: A router is used to route between LAN and GPRS having the MTU for the GPRS interface set to 1 448 and the MTU for the LAN interface set to 1 500, which is the default for Ethernet. ForwardBufferMemory has not been changed from its default value 74 240. Thus, the resulting value should be at least as large as 50 and not larger than 290 depending on the amount of data in each packet. The closer the average data size of the packets gets to the maximum MTU of the networks connected, the smaller is the number to be chosen for the NumForwardPackets parameter.

SackOpts (XP only, optional)

Recommendations: This parameter should stay at default value 1 and is only listed here since it was referred to earlier.

NOTE 3: If this parameter is not in the Registry but Tcp1323Opts is enabled, the referred Windows operating systems will default to supporting SACK.

Tcp1323Opts *(Vista, XP optional)*

Recommendations: Window scaling can be enabled but timestamp options should be disabled to be able to use header compression. Thus, the parameter should be set to 1 on client and server side.

NOTE 4: If no header compression is available in the network, time stamping should be enabled to be able to calculate a better RTT estimation.

TcpDelAckTicks (*Vista, XP optional)*

Recommendations: This parameter should be set to 0 for programs sending data packets interactively (Interactive Traffic; e.g. SSH, telnet), otherwise (Bulk Traffic; e.g. FTP, HTTP) left at default value 2 (200 milliseconds).

TcpInitialRTT *(XP only, optional)*

Recommendations: The initial value of 3 seconds is most probably too long for the current GPRS implementation (depends on the MTU), causing the transmission to slow down before it even started completely. Set it to a reasonable value like the time for a 1 500 byte ping.

NOTE 5: If the selected value is to small, for example smaller than the time needed for a 3WHS, each TCP connection request would cause at least one retransmission. On the other hand, setting the parameter to a relatively high value could in the case of a lost packet cause noticeable delays for the user.

TcpMaxConnectRetransmissions *(XP only, optional)*

Recommendations: The optimal setting for this parameter is dependant on many environmental influences and on the mobility of the user. In non stationary and in environments causing a high packet loss rates in general, it might make sense to use more than two attempts. In general, this parameter can stay at its default value.

TcpUseRFC1122UrgentPointer *(Vista, XP optional)*

Recommendations: This can be used if urgent data need to be signalized. Nevertheless, it is recommended to open two separate sockets with one handling urgent data and one handling non-urgent data.

TcpWindowSize *(XP only, optional)*

Recommendations: This parameter has a big impact on overall GPRS performance; therefore it should be handled with caution. To determine a reasonable value for the mentioned factor the MSS should be multiplied with, the following equation can be used:

$$TcpWindowSize = n * MSS$$

where n should be set to a natural number being bigger or equal to four. Here, n should be chosen so that the resulting product equals the bandwidth-delay product. Note that bandwidth, as well as delay, are no static values in a GPRS network. Furthermore, these values can change quite a lot, e.g. due to different data communication routes caused by movements of the mobile device.

NOTE 6: Usable information for the round-trip-time (RTT) can only be determined from the server side. The RTT can not be compared to a value acquired with a "ping" command, since the estimated value is also dependant on the amount of data sent. If it is impossible to test RTT on server side, a good value for 3+1 mobile devices is 17 520. Also, as some tests have shown, the value n needs not always to be an even number.

NOTE 7: Windows 2000 does not use the configured TCPWindowSize registry parameter when accepting a connection (SYN-ACKing) if the parameter is configured per interface and if the value is equal to or greater than 64 240 (it uses a window size of 17 520 instead, if you are using Ethernet). The cause for this is, that the TCP connection accept functionality does not correctly parse the window size if you configure the parameter per interface. To resolve this issue, the TCPWindowSize value should be set globally or a value smaller than 64 240 should be used. Since this should be the case when following the recommendations given here, this issue should not cause any problems.

7 Changes commonly applied by Software provided by Network Operators (Windows XP)

This clause provides a list of changes to local Windows XP TCP IP configuration parameter settings made by certain drivers or software provided by network operators.

The main intention of such software is to allow network operator's customers to easily establish and maintain an Internet connection while often also tuning the TCP IP Stack implementation of the customer's computer with respect to the operator's network. These changes can happen e.g. during installation of the respective software or when running the software and altering settings on a user interface level, e.g. configuration Dashboard settings dialogue.

The results provided in the following are exemplary, are based on a survey taken in Europe in the beginning of 2007 and provide a snapshot of the situation within five European countries when using such software together with a data card in order to access and utilize 3G networks.

The following table provides information about the existence of performance optimizer clients being integrated in the software referred above.

Table 2: Information of Windows XP software provided by network operators with respect to optimizer clients

Country	Network Operator	Optimizer Client
A	A1	N
	A2	N
	A3	N
	A4	N
B	B1	Y
	B2	N
	B3	Y
	B4	Y
C	C1	N
	C2	N
D	D1	N
	D2	N
	D3	N
	D4	Y
E	E1	Y
	Ê2	Y
	E3	N
	E4	N
	E5	N

The changes to local Windows XP TCP IP configuration parameter settings made by the respective network operator software are listed by country in the following clauses.

7.1 Exemplary Country A

Changes to TCP parameter configuration applied by software provided for the Windows XP operating system by network operators in country A.

Table 3: TCP parameter changes by network operator software in country A

	Country A			
Relevant Registry Keys	**A1**	**A2**	**A3**	**A4**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]				
SackOpts	1	1	1	1
Tcp1323Opts	2	1	1	-
TcpMaxConnectRetransmissions	5	-	-	-
TcpMaxDupAcks	3	-	-	2
TcpWindowSize	65535	128480	65535	16384
GlobalMaxTcpWindowSize	131072	-	133000	-
EnablePMTUBHDetect	-	-	-	-
EnablePMTUDiscovery	-	-	-	-
DefaultTTL	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]				
MTU	-	-	-	-
TcpWindowSize	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Protocols\1]				
PPPProtocolType	-	-	-	-
ProtocolMTU	-	-	-	-
ProtocolType	-	-	-	-

	Country A			
Relevant Registry Keys	**A1**	**A2**	**A3**	**A4**
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]				
MaxConnectionsPer1_0Server	-	-	-	-
MaxConnectionsPerServer	-	-	-	-

7.2 Exemplary Country B

Changes to TCP parameter configuration applied by software provided for the Windows XP operating system by network operators in country B.

Table 4: TCP parameter changes by network operator software in country B

	Country B			
Relevant Registry Keys	**B1**	**B2**	**B3**	**B4**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]				
SackOpts	1	1	1	1
Tcp1323Opts	1	-	3	3
TcpMaxConnectRetransmissions	-	-	-	5
TcpMaxDupAcks	-	-	-	-
TcpWindowSize	65535	16384	65560	131072
GlobalMaxTcpWindowSize	133000	-	-	131072
EnablePMTUBHDetect	-	-	-	-
EnablePMTUDiscovery	-	-	-	-
DefaultTTL	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]				
MTU	-	-	-	-
TcpWindowSize	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Protocols\1]				
PPPProtocolType	-	-	-	-
ProtocolMTU	-	-	-	-
ProtocolType	-	-	-	-
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]				
MaxConnectionsPer1_0Server	-	-	-	-
MaxConnectionsPerServer	-	-	-	-

7.3 Exemplary Country C

Changes to TCP parameter configuration applied by software provided for the Windows XP operating system by network operators in country C.

Table 5: TCP parameter changes by network operator software in country C

	Country C	
Relevant Registry Keys	**C1**	**C2**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]		
SackOpts	1	1
Tcp1323Opts	3	1
TcpMaxConnectRetransmissions	5	-
TcpMaxDupAcks	-	-
TcpWindowSize	131072	128480
GlobalMaxTcpWindowSize	131072	-
EnablePMTUBHDetect	-	-
EnablePMTUDiscovery	-	-
DefaultTTL	-	-

	Country C	
Relevant Registry Keys	**C1**	**C2**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]		
MTU	-	-
TcpWindowSize	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Protocols\1]		
PPPProtocolType	-	-
ProtocolMTU	-	-
ProtocolType	-	-
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]		
MaxConnectionsPer1_0Server	-	-
MaxConnectionsPerServer	-	-

7.4 Exemplary Country D

Changes to TCP parameter configuration applied by software provided for the Windows XP operating system by network operators in country D.

Table 6: TCP parameter changes by network operator software in country D

	Country D			
Relevant Registry Keys	**D1**	**D2**	**D3**	**D4**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]				
SackOpts	1	1	1	1
Tcp1323Opts	1	-	3	3
TcpMaxConnectRetransmissions	-	-	-	5
TcpMaxDupAcks	-	-	-	-
TcpWindowSize	65535	16384	146000	131072
GlobalMaxTcpWindowSize	133000	-	-	131072
EnablePMTUBHDetect	-	-	-	-
EnablePMTUDiscovery	-	-	-	-
DefaultTTL	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]				
MTU	-	-	-	-
TcpWindowSize	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Protocols\1]				
PPPProtocolType	-	-	-	-
ProtocolMTU	-	-	-	-
ProtocolType	-	-	-	-
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]				
MaxConnectionsPer1_0Server	-	-	-	-
MaxConnectionsPerServer	-	-	-	-

7.5 Exemplary Country E

Changes to TCP parameter configuration applied by software provided for the Windows XP operating system by network operators in country E.

Table 7: TCP parameter changes by network operator software in country E

	Country E				
Relevant Registry Keys	**E1**	**E2**	**E3**	**E4**	**E5**
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]					
SackOpts	1	1	1	1	1
Tcp1323Opts	1	3	-	1	-
TcpMaxConnectRetransmissions	-	5	-	-	-
TcpMaxDupAcks	-	-	-	-	-
TcpWindowSize	65535	131072	16384	128480	42000
GlobalMaxTcpWindowSize	133000	131072	-	-	-
EnablePMTUBHDetect	-	-	-	-	-
EnablePMTUDiscovery	-	-	-	-	-
DefaultTTL	-	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces]					
MTU	-	-	-	-	-
TcpWindowSize	-	-	-	-	-
[HKLM\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\Protocols\1]					
PPPProtocolType	-	-	-	-	-
ProtocolMTU	-	-	-	-	-
ProtocolType	-	-	-	-	-
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]					
MaxConnectionsPer1_0Server	-	-	-	-	-
MaxConnectionsPerServer	-	-	-	-	-

8 Changes commonly applied by Software provided by Network Operators (Windows Vista)

For further study: Changes to local Windows Vista TCP IP configuration parameter settings made by the respective network operator software.

Annex A:
Former Recommendations

The following citation was formally to be found in the TS 102 250-5 [4]. It was removed giving consideration to the fact that software provided by network operators for different operating systems in order for the end-user to access the operators network commonly applies changes to the TCP IP Stack.

Furthermore and with respect to the fact these changes might differ from county to country and from operator to operator, such changes might also influence the respective operating systems in different ways. Thus, simulation of the majority of customers can currently not be performed as easily as formally stated in the TS 102 250-5 [4] document:

"(…) For all data measurements TCP settings may be chosen at will.

If the measurements shall be used for comparison with other networks the following settings shall be used on the measurement client (based on the assumption, that the majority of the customers will use Microsoft WINDOWS XP Professional SP1 English):

Maximum Segment Size between 1 380 bytes and 1 460 bytes

TCP RX Window Size = 16 384 bytes

SACK enabled

ECN disabled

TCP Window Scaling disabled

TCP Timestamping disabled

PMTU Discovery disabled (but DF-bit set)

TCP Fast Retransmit

TCP Fast Recovery enabled

Delayed ACK enabled (200 ms)

NOTE 1: The recommended TCP settings represent one of the possible (out-of-the-box) implementations of a common operating system of a client. The reason why this option was chosen was due to the fact that these are closer to the "default" user settings.

*These settings are not and should definitely not be considered as the preferred or optimized TCP settings over 2.5/3 G. A good reference for optimized TCP parameters over cellular networks like 2.5/3 G is the RFC 3481 [*11*] which is of the Best Current Practise (BCP) category in the IETF published on February of 2003.*

NOTE 2: Although the same TCP parameters may be used for benchmarking purposes, when different OSs are used in the tests, different results maybe obtained. This is due to the different implementations of the TCP/IP stack in the different OSs. This needs to be considered when comparing the results from a benchmarking exercise especially when the client and/or server OSs of the compared networks are not the same. This is a limitation which should not be overlooked, and a possible solution is to use the same version of the OSs in the client, as well as the server for all networks compared in a benchmark campaign (this does not imply that the OS of the client must be the same as the server).

NOTE 3: Proxy servers installed in the networks IP core network may act as the TCP peer instead of the application server the tests are performed against.

Measurements with other settings may not be called conforming to the present document. There is no preference concerning the used operating system as long as these settings are used. (…)

The TCP settings of the server tested against should also be recorded. Since the number of host operating systems for internet servers is larger than on the client side, no detailed recommendation concerning the TCP settings of the server is given. However, the TCP IP Stack of the reference server should at least be capable of the following:

Maximum Segment Size between 1 380 bytes and 1 460 bytes

TCP RX Window Size > 4 096 bytes

SACK enabled

TCP Fast Retransmit

TCP Fast Recovery enabled

Delayed ACK enabled (200 ms)

(…)"

History

Document history		
V1.1.1	October 2007	Publication