Nordic Connect Managed

Service Description
For release 2.6.4

Table of Content

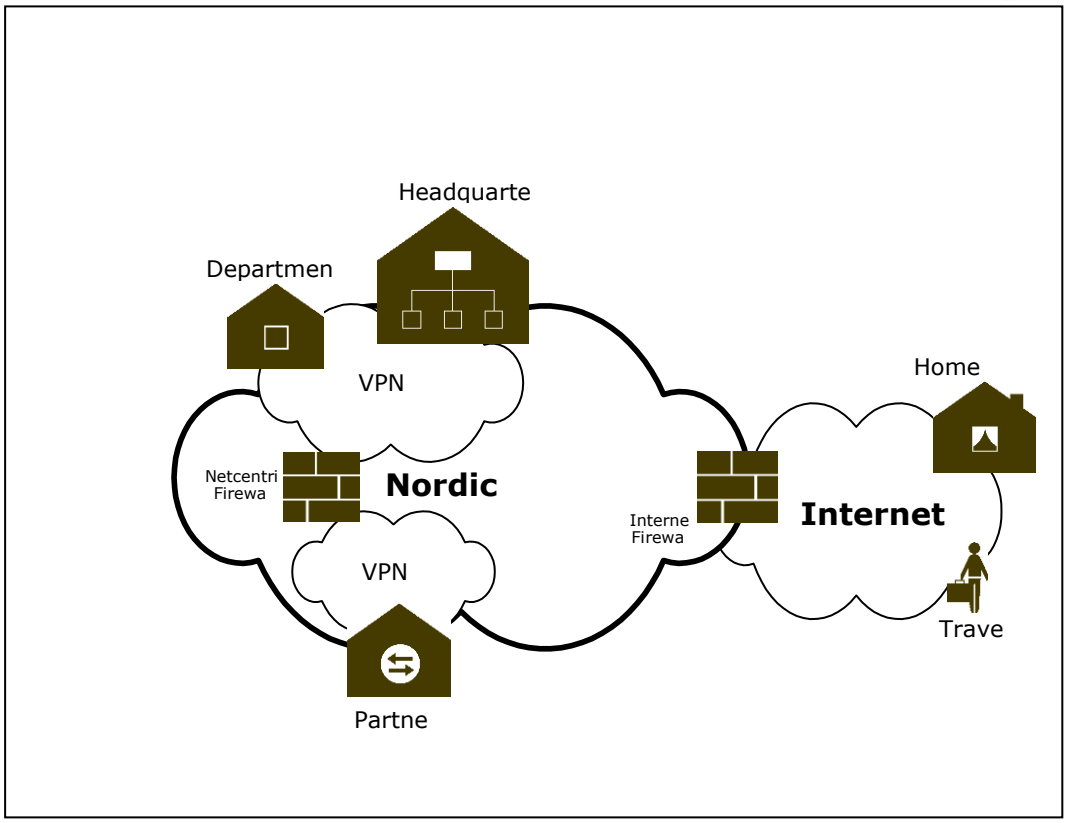
1. Introduction

This document is subject to change. Telenor reserves the right to alter the content of this document with the purpose to make further developments, improvements and adjustments which do not reduce the quality of the services and products. The legally binding version of this document is always the latest official release from Telenor.

Nordic Connect is an IP VPN service based on BGP/MPLS described in IETF RFC 2547. It is targeted on large corporations, mid-size enterprises and small businesses in the Nordic countries.

Some key characteristics of the Nordic Connect services are:

- *Fully meshed connectivity*
  Each site can access services on all other sites in the VPN via one access line.
- *Differentiated access services*
  Access services span from basic connectivity service utilising low cost broadband access networks, to redundant gigabit solutions based on customer-dedicated optical fibers.
- *Mobile Access*
  Mobile access to Nordic Connect can be used to increase flexibility and mobility. Access via Telenors Mobile data network can be used for teleworkers, M2M-solutions, easy moveable customer sites or as complement to fixed access.
- *Nordic availability*
  Nordic Connect offers a single point of contact for provisioning and support across all Nordic countries, plus local support in each country.
- *Quality of Service*
  Delay sensitive traffic on the network can be given the necessary priority. Hence, optimizing network usage for the types of applications within an organization.
- *Multi-VPN*
  Each site can have access to several separate VPNs via the same access line. A customer can for example have one VPN for each of the company divisions, distinct VPNs for each of the company suppliers and an Internet VPN.
- *Differentiated SLAs*
  Each access line is delivered with a standard Service Level Agreement (SLA) adapted to the targeted market segment. Improved SLAs are available as an additional service for locations with special requirements.
- *Broad range of add on services*
  A broad range of add on services are available, in addition to QoS, Multi-VPN and SLAs. Examples are Internet firewall, remote office solutions, point-to-point encryption, dynamic routing, hub-and-spoke network topologies, etc.
- *Choice of available access technologies*
  The Nordic Connect service makes use of the locally available access technologies to deliver the desired service.
- *Continuous surveillance*
  Availability of the Nordic Connect service is under constant monitoring from Telenor's network management centre.
- *Web based reports*
  The web based statistics and monitoring tool WEBline is included in the service. WEBline gives access to administration, network overview and statistics for each site in the customer network.



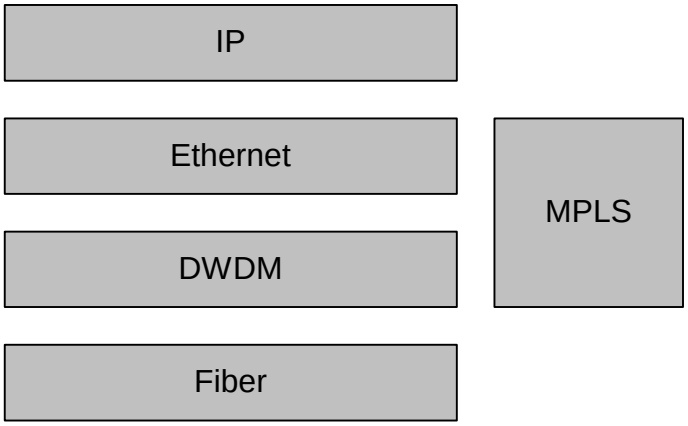
Figur 1 Customer with Nordic Connect solution

2. Technology

The VPN-functionality in Telenor's networks is based on MPLS (Multi Protocol Label Switching). MPLS provides strong integrity and security as each VPN has separate routing tables. Traffic in one VPN is totally inaccessible for users in other VPNs. Hence, security against intrusion from undesirable parties is very high.

MPLS is a very flexible technology. A VPN is defined as a logical function in MPLS. Hence, sites can be added, removed and changed in an easy manner.

Telenor's core-network for data communications is built based on a layered model similar to the OSI model. The layered model of Telenor's core network is shown in the figure under:



Figur 2: Layered model of Telenor's network

The core of the network is built on Telenor's fiber infrastructure. Redundancy on this layer is achieved by utilizing physical diversity.

The optical layer is built using Dense Wavelength Division Multiplexing (DWDM). DWDM is a technology where light of different wavelengths (colours) is multiplexed onto the same fiber in order to maximize transmission capacity. By the use of links with high transmission capacity, traffic can be routed with minimum delay.

Telenor uses Gigabit Ethernet and MPLS to link the optical layer with the IP layer. These are switching technologies, which is a guarantee for speed and performance in the network.

All customer VPNs are defined as separate VPNs in the Telenor network. On Ethernet links in the access network, traffic in different VPNs is separated by 802.1Q VLANs. On MPLS links in the core network, IP-packets are separated by the use of MPLS labels. The mapping from VLAN id to MPLS label and vice versa is performed in Telenors Provider Edge (PE) routers.

MPLS is a switched technology. Hence, the core of Telenor's network represents one IP hop, and can be seen as one virtual router. In a traditional router all routes are defined in one global routing table. In Telenor's core network, every PE router maintains separate routing tables (VRF – Virtual Routing and Forwarding instance) for every VPN that is present in the router. The security in such a VPN is similar to the security in a system where VPNs terminate in separate physical routers.

The network is designed to handle disruptions between nodes in a fast and effective way. MPLS uses predefined routes in the network to ensure fast reaction when there is a disruption in the underlying layer.

The MPLS network is redundantly connected to Telenors Mobile data network to enable mobile access to Nordic Connect. Dedicated APNs are used to direct data traffic from the mobile data network to the Nordic Connect network. IP-tunnels (GRE) are used to separate customer connections to the customer VPN. Since the mobile network is directly connected to the MPLS network, the traffic from the mobile connections are not using any Internet connections.

3. Service Description

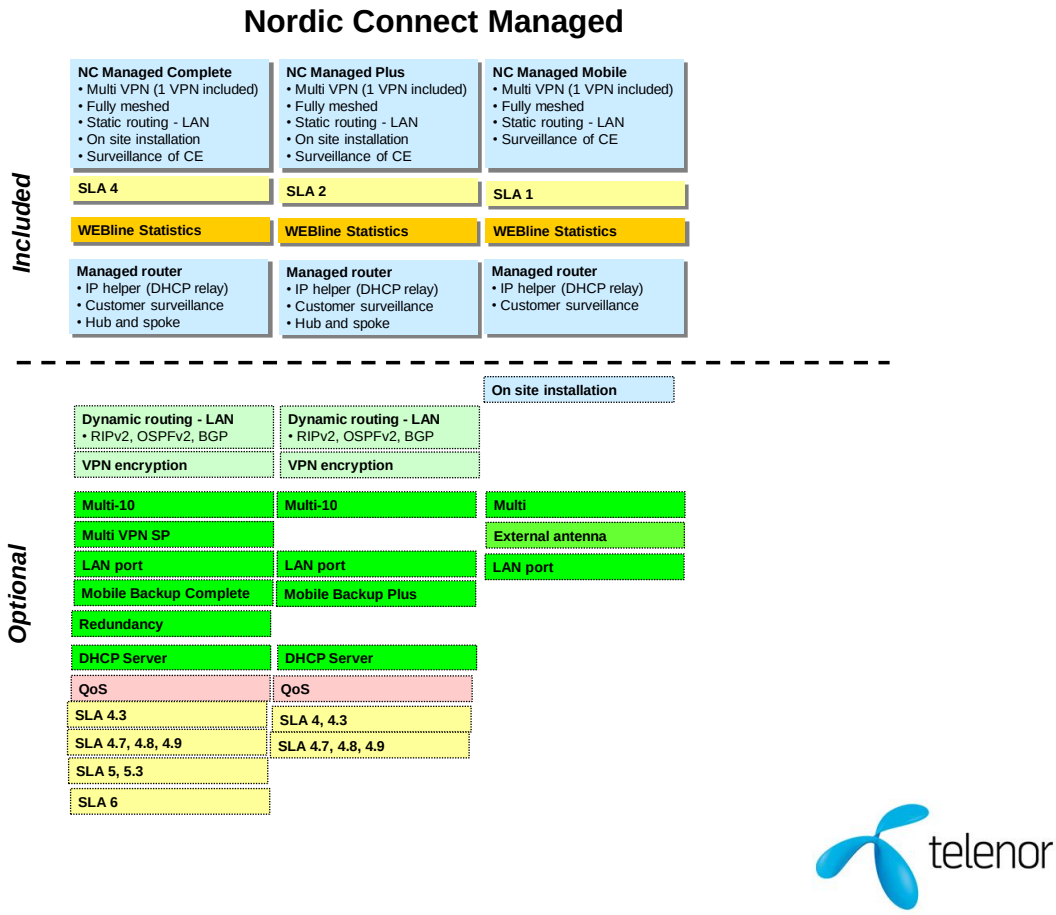
The figure below gives a brief overview of the Nordic Connect service. The service comes in two different varieties:

- Nordic Connect Managed
- Nordic Connect Partner

Nordic Connect Managed is a fully managed service. The service includes provisioned and managed router from Telenor. Nordic Connect Managed is aimed at customers wanting to buy a turnkey network solution from one contractor.

Nordic Connect Partner is a partly managed service. The service includes a provisioned and managed switch from Telenor. Nordic Connect Partner is aimed at customers and ASPs who wish to manage their own router or partners providing managed services, including router functionality.

This document is the Service Description for the service Nordic Connect Managed.



Figur 3 Overview of the service Nordic Connect Managed

Nordic Connect Managed exists in three different service bundles:

- ***Nordic Connect Managed Complete*** offers the full range of features and additional options. Access types are always symmetric (leased line, fiber, radio), with bandwidths up to 10 Gbps.
- ***Nordic Connect Managed Plus*** supports the same set of features and additional options as Complete except redundancy and Multi SP. Access types can be asymmetric or symmetric and are based on xDSL.
- ***Nordic Connect Managed Mobile*** allows Nordic Connect customers to connect remote LAN sites to their VPN via the mobile packet data network. The service can also be deployed as

semi-mobile, i.e. customers can move CE equipment from one site to another provided it is stationary during use.

Notes:

1) On-site installation is an option for NC Managed Mobile in Norway and Denmark. In Sweden this is always included.
2) Maximum IP MTU size for Nordic Connect Managed Mobile is 1476. For fixed access types (xDSL, LL, fiber) it is 1500.

3.1 Area of Coverage

Nordic Connect is available in Norway, Sweden and Denmark. On request, the service can possibly be delivered on Spitsbergen.

Through Telenor partnership with Elisa we can also provide access to Nordic Connect in Finland. For more information about the service available in Finland, see separate document “Nordic Connect Managed Service Description Annex 1- Finland”.

3.2 Bandwidth and Access Technology

3.2.1 Introduction

The tables in chapter 3.2.1 - 3.2.4 provides an overview of the different access types that are used to provide access to Nordic Connect in Norway, Sweden and Denmark. The column on the left shows the nominal Product IP speed, and for each service bundle the corresponding shaping speed used for traffic shaping in the CE and PE router is listed. Dependant of access technology this is either identical to the nominal Product speed, or there is a deviation.

The reason for using a shaping speed that is lower than the theoretical maximum achievable speed is to avoid that packet loss occurs in the underlying transmission layer. By minimizing packet loss in the transmission path, shaping ensures maximum throughput for the actual payload.

Selection of the appropriate shaping speed is not only dependant on access type, but also on the characteristics of the network elements deployed to provide the access service. Since these can be different in Norway, Sweden and Denmark, national differences can occur.

3.2.2 Norway, fixed line access

NC Product speed	Managed Plus		Managed Complete			
	Access type	Shaping speed	Access type 1	Shaping speed	Access type 2	Shaping speed
700/200k	ADSL	700k/200k				
1M/300k	ADSL	1M/300k				
2M/350k	ADSL	2M/350k				
4M/450k	ADSL	3,9M/450k				
6M/480k	ADSL	5,8M/480k				
8M/530k	ADSL	7,7M/530k				
12M/630k	ADSL	11,6M/630k				
12M/700k	VDSL	12M/700k				
20M/3M	VDSL	20M/3M				
25M/8M	VDSL	25M/8M				
30M/8M	VDSL	30M/8M				
64k			LL	56k		
512k	SHDSL	500k	LL	450k		
1M	SHDSL	1.000k	LL	900k		
2M	SHDSL	1.850k	LL	1.800k		
4M	SHDSL	3,7M	LL	4M		
8M	SHDSL	7,4M				
10M			LL	9,5M	Fiber	10M
20M			LL	19M	Fiber	20M
40M			LL	40M	Fiber	40M
100M			LL	90M	Fiber	97M
200M			LL	200M	Fiber	200M
300M			LL	270M	Fiber	300M
400M			LL	400M	Fiber	400M
600M			LL	570M	Fiber	600M
1000M			Fiber	980M	Optical channel	980M
2G			Fiber	2000M	Optical channel	2000M
4G			Fiber	4000M	Optical channel	4000M
6G			Fiber	6000M	Optical channel	6000M
10G			Fiber	9800M	Optical channel	9800M

Table 1 Bandwidths and Access Technologies in Norway

Note:

SHDSL accesses are by default delivered using the minimum number of wire pairs required for the selected access speed, as specified by the G.SHDSL standard. Other combinations of wire pairs are

supported on Norwegian SHDSL accesses as an optional add on service. This is described in more detail in chapter 3.6.9.

3.2.3 Sweden

NC Product speed	Managed Plus		Managed Complete			
	Access type	Shaping speed*	Access type 1	Shaping speed	Access type 2	Shaping speed
512k/200k	ADSL					
2M/350k	ADSL					
4M/450k	ADSL					
8M/530k	ADSL					
12M/630k	ADSL					
16M/630k	ADSL					
2M/1,5M	ADSL.m					
4M/1,5M	ADSL.m					
8M/1,5M	ADSL.m					
10M/1,5M	ADSL.m					
16M/1,5M	ADSL.m					
20M/3M	VDSL.m	20/3M				
25M/8M	VDSL.m	25/8M				
30M/8M	VDSL.m	30/8M				
2M			SHDSL/VDSL/Fiber	1,85M	Ethernet	1,85M
4M			SHDSL/VDSL/Fiber	3,7M	Ethernet	3,7M
6M			SHDSL/Fiber	5,55M		
8M			SHDSL/VDSL/Fiber	7,4M	Ethernet	7,4M
10M			VDSL/Fiber	9,25M	Ethernet	9,25M
20M			Fiber	18,5M	Ethernet	18,5M
40M			Fiber	40M	Ethernet	40M
100M			Fiber	100M	Ethernet	100M
200M			Fiber	200M		
400M			Fiber	400M		
600M			Fiber	600M		
1000M			Fiber	1000M		
2G			Fiber	2000M		
4G			Fiber	4000M		
6G			Fiber	6000M		
10G			Fiber	9800M		

* In Sweden bandwidth shaping is not used on ADSL/VDSL access types. Product IP speed in downstream direction is secured by setting higher speed on the access compensating for overhead added by ADSL layer.
For ADSL and ADSLm access NC Product Speeds in upstream direction are minimum levels and higher bandwitdths may be available. NC products based on ADSL.m accesses are shaped in upstream direction to 2 Mb.
SHDSL may be used as access form in some situations instead of ADSL and ADSL.m accesses up to a NC Product speed of 8Mb downstream.

Table 2 Bandwidths and Access Technologies in Sweden

3.2.4 Denmark

NC Product speed	Managed Plus	
	Access type	Shaping speed*
Flex ADSL	ADSL	≤20M/2M
Flex VDSL	VDSL	≤40M/10M

NC Product speed	Managed Complete			
	Access Type 1	Shaping speed	Access type 2	Shaping speed
10M	Radio / Fiber	10M		
20M	Radio / Fiber	20M		
40M	Radio / Fiber	40M		
100M	Radio / Fiber	100M		
200M	Fiber	200M		
400M	Fiber	400M		
600M	Fiber	600M		
1G	Fiber	1.000M		
2G	Fiber	2.000M		
4G	Fiber	4.000M		
6G	Fiber	6.000M		
10G	Fiber	10.000M		

* NC products based on ADSL and VDSL in Denmark will always be delivered as Flex DSL, which means that Telenor will deliver the best possible bandwidth that the line speed provides (best effort). Maximum line speed will be measured on the installation date and the highest possible shaping speed will be set for each DSL line. Depending on line length and quality of the DSL access line the shaping speed may vary from different DSL installations.

Table 2 Bandwidths and Access Technologies in Denmark

3.2.5 Mobile Access

Mobile access to Nordic Connect is being used for the Services Nordic Connect Managed Mobile and Nordic Connect Mobile Backup.

Table 3 Access Technologies for Managed Mobile and Mobile Backup

Mobil Network	Mobil Data bærer	Maks. teoretisk Båndbredde		Typisk Båndbredde [2)]	
		Downstream	Upstream	Downstream	Upstream
GSM/GPRS	EDGE [1)]	236,8k	50k – 75k	100 - 200k	50 – 75k
UMTS (3G)	3G	384k	64k	250 - 350k	50 - 60k
UMTS (3G)	HSDPA	3,6M	384k	0,5 – 1,5M	250 - 360k
UMTS (3G)	HSUPA	7,2M	2M	0,5 – 3M	0,5 – 1,5M
LTE (4G)	LTE	71M	43M	2 – 71M	2 – 43M

1) Typical Bandwidth will vary based on coverage and simultaneous users.

Mobile access to Nordic Connect is using the best available bandwidth provided by the mobile network at the CE location. Available bandwidth can change over time due to utilisation in the mobile network. Therefore bandwidth and performance (delay etc.) cannot be guaranteed.

The mobile subscription is included in the Nordic Connect Managed Mobile and Nordic Connect Mobile Backup services. Usage is also included for Mobile Backup.

The mobile subscription is suspended for voice traffic and roaming. The roaming suspension means that the Mobile access cannot be used in other countries or mobile networks.

Mobile coverage on-site is the responsibility of the customer and must be acknowledged with customer during sales phase.

3.2.6 Subscription types for Managed Mobile

3.2.6.1 Norway

NC Managed Mobile is based on a Mobile Broadband subscription type with a fixed monthly price that includes packets with 50, 100 and 150 Gigabyte of data. Usage beyond 150 Gigabyte is billed per consumed Mbytes.

3.2.6.2 Sweden

Nordic Connect Managed Mobile includes Mobile Broadband access in the fixed monthly recurring charge.

3.2.6.3 Denmark

NC Managed Mobile is based on a Mobile Broadband subscription type with a fixed monthly price that includes 10 Gigabyte of data. If usage exceeds 10 Gigabyte in a month the bandwidth will be lowered to max. 256 kbps for the rest of the month.

Telenor can send an alert to the customer via SMS or e-mail when the traffic volume exceeds a predefined threshold. Only one alert is generated per month (measuring period), and the feature must be activated by the customer via Webline by entering the required contact information.

3.3 Interfaces and Protocols – LAN port

The network protocol is IP version 4.

Certain derogations to this table can occur due to choice of CE router

NC product	Interface type	Connector	Protocols	LAN-port setting	
				Default	Optional
NCM Mobile	Fast Ethernet, untagged/tagged	RJ-45	IEEE 802.3u IEEE 802.3i IEEE 802.1Q	100/Full duplex	Auto/Auto 10/Full duplex 10/Half duplex
NCM Basic	Fast Ethernet, untagged	RJ-45	IEEE 802.3u IEEE 802.3i	100/Full duplex	Auto/Auto 10/Full duplex 10/Half duplex
NCM Plus	Fast Ethernet, untagged/tagged	RJ-45	IEEE 802.3u IEEE 802.3i IEEE 802.1Q	100/Full duplex	Auto/Auto 10/Full duplex 10/Half duplex
NCM Complete, ≤ 100M	Fast Ethernet, untagged/tagged	RJ-45	IEEE 802.3u IEEE 802.3i IEEE 802.1Q	100/Full duplex	Auto/Auto 10/Full duplex 10/Half duplex
NCM Complete, 200M – 1G	GE Fiber Untagged/tagged	GE SFP LC connector with SX transceiver (multi mode)	IEEE 802.3z IEEE 802.1Q	Auto/Auto	None
NCM Complete, 2G – 10G	10GE Fiber, untagged/tagged	10GE XFP LC connector with SR transceiver (multi mode)	IEEE 802.3ae IEEE 802.1Q	Auto/Auto	None

Table 4 Interfaces and Protocols for Nordic Connect

IEEE 802 protocols:

IEEE 802.3i - 10BASE-T, 10 Mbit/s over twisted pair

IEEE 802.3u - 100BASE-TX, 100BASE-FX Fast Ethernet at 100 Mbit/s w/auto-negotiation

IEEE 802.3z - 1000BASE-X, Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s

IEEE 802.3ae – 10Gbase, 10 Gbit/s Ethernet over optical fiber

IEEE 802.1Q – Standard for VLAN tagging

3.4 Service Features

The following service features are supported in Nordic Connect Managed:

Group	Function	Mobile	Plus	Complete
VPN functionality	VPN topology - full mesh	Included	Included	Included
	VPN topology – hub & spoke	-	Included	Included
	Routing protocol – static	Included	Included	Included
	Routing protocol – dynamic	-	Optional	Optional
Encryption	VPN Encryption	-	Optional	Optional
Managed router	Managed router	Included	Included	Included
	DHCP relay	Included	Included	Included
	DHCP server in CE	Included	Included	Optional
	SNMP read access	Included	Included	Included
Multi VPN	Multi VPN	Optional	Included	Included
	Multi 10	-	Optional	Optional
	Multi SP	-	-	Optional
	Extra VPN Access	Optional	Optional	Optional
Extra LAN port	Extra LAN port	Optional	Optional	Optional
QoS	QoS 3 Classes	-	Optional [2)]	Optional
	QoS 4 Classes	-	Optional [2)]	Optional
	Custom QoS	-	Optional [2)]	Optional
	Weight profile implementation [4)]			
SLA	SLA level 1	Included	-	-
	SLA level 2	-	Included	-
	SLA level 4	-	Optional	Included
	SLA level 4.3	-	Optional	Optional
	SLA level 4.7	-	Optional	Optional
	SLA level 4.8	-	Optional	Optional
	SLA level 4.9	-	Optional	Optional
	SLA level 5	-	-	Optional
	SLA level 5.3	-	-	Optional
	SLA level 6	-	-	Optional
Statistics	Webline statistics	Included	Included	Included
Backup [3)]		-	Optional	Optional
Redundancy	Redundant access line	-	-	Optional
SHDSL wire pairs	Extra wire pairs	-	Optional	-l

Notes:

1) Basic is available in Sweden only
2) Supported in Norway and Denmark
3) For details on availability of Backup see chapter 3.6.7.1
4) Applies on the customer level independent of access product.

Table 5 Service Features for Nordic Connect Managed

3.5 Standard Service Features

Standard service features are included in the service, and can be activated at installation time without additional cost elements being added. If the standard features are changed or activated at a later stage, a fee will be charged.

3.5.1 Customer VPN

Service feature	Mobile	Plus	Complete
1 VPN	Included	Included	Included
Multi VPN	Optional	Included	Included

Each customer network is implemented as a solitary VPN. Connection to one VPN is a standard service feature of every Nordic Connect access line.

Nordic Connect Managed Plus and Complete accesses supports connection to a maximum of 5 VPNs over the same access line. For Nordic Connect Managed Mobile accesses the support for connection to additional VPNs is an optional add-on service described in section 3.6.3.1.

Connection to VPNs in addition to the one included on every access line is an optional add-on service described in section 3.6.4.

3.5.2 Fully Meshed VPN Topology

Mobile	Plus	Complete
Included	Included	Included

Nordic Connect offers a WAN solution that is realized with a full mesh topology. Full mesh is the default topology if Hub-Spoke is not actively chosen. This offers flexible and scalable VPN functionality without the need to establish and administer connections between sites.

3.5.3 Hub-Spoke VPN topology

Mobile	Plus	Complete
Not available	Included	Included

Nordic Connect offers a WAN solution that is realized with hub-spoke topology as an option. That is, each site in the network can be configured either as a hub or a spoke type location. Each spoke type location can only communicate directly with one or several hub type locations.

The realization of a hub-spoke network solution demands a Multi-VPN solution at the Hub-location. The Hub-location is configured with two VPN-accesses: Hub-in and Hub-out. Traffic from the spoke will be routed to Hub-in (this is the only route the spoke knows). Traffic from the hub to the spoke will be routed through the Hub-out. This means that all traffic to/from spokes are separated in two different VLAN's at the router LAN interface. If the customer wants to prevent all traffic between the spokes, a firewall must be installed between the Hub-in and Hub-out VLAN's. At present, Telenor can only deliver a customer located firewall in Norway.

Another hub-spoke design can be realized by the use of a Net-Centric Firewall (NFW). In this solution the NFW is inserted between two VPN's. One of the VPN's connecting the member locations with a hub-spoke infrastructure. The NFW acts as a hub in the VPN. The other VPN can be implemented with a full-mesh infrastructure. This means that the spokes in the network can communicate only with one or several hubs. Hub-Spoke is implemented per VPN. It is therefore possible to have a Multi-VPN solution with one VPN-access fully meshed and one VPN-access with Hub-Spoke.

.

3.5.4 Static Routing LAN

Mobile	Plus	Complete
Included	Included*	Included

The standard routing mechanism between the customer LAN and Nordic Connect is static routing.

The customer can use both private and public IP addresses in Nordic Connect with some restrictions.

Telenor reserved IP addresses:
Telenor uses RFC1918 IP addresses for addressing of the PE-CE link. These address ranges are 172.20.0.0 – 172.31.255.255 and 10.64.0.0 – 10.79.255.255. The customer is free to choose which of the two ranges Telenor should use for PE-CE link addresses. If the range is not specified, addresses from the range 172.20.0.0 – 172.31.255.255 will be used as default. The chosen PE-CE link address block will be visible from the customer location, and will be part of the total VPN address scheme. It is important that the customer refrain from using this address block in the LAN's connected to the VPN's.

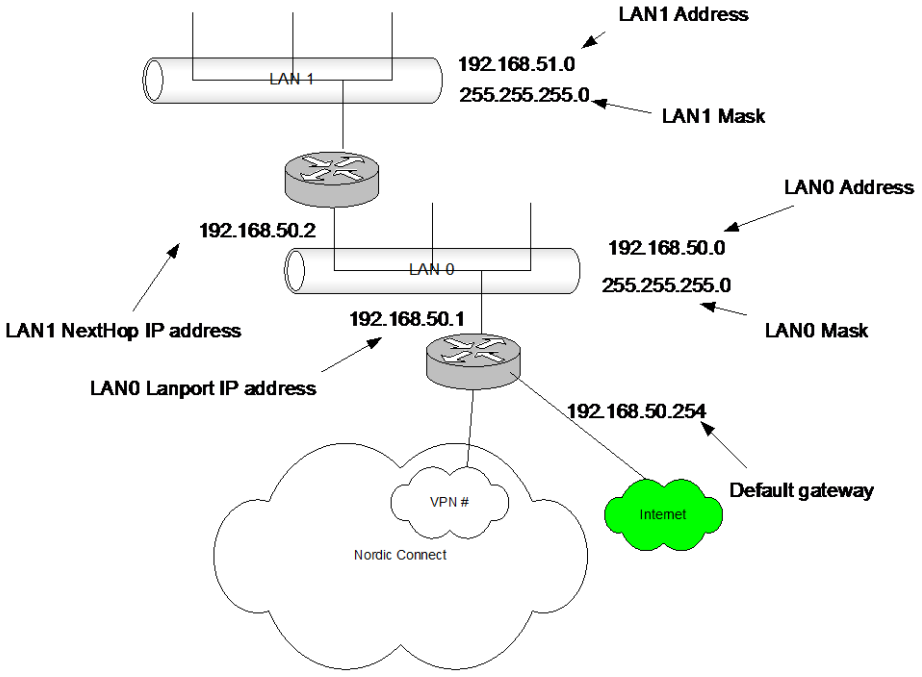
The usual customer location has one LAN (subnet). In some cases, however, the customer site is composed of a LAN (subnet) with one or several underlying LANs (subnets) separated with routers. If this is the case, the customer must state the routes for all these LANs.

Routes must be stated for each particular VPN in Multi-VPN solutions.

Figure 4 gives an example of a customer site with a subnet (LAN0), and one underlying subnet (LAN1). The figure states all the IP addresses that must be specified.

Note:

*) xDSL access lines in Norway supports up to 6 underlying subnets.



Figur 4 LAN routing for a Nordic Connect Customer

- ***LAN0 Address/LAN0 Mask***. Address and network mask specifying the address range of LAN0.
- ***LAN0 LANport IP address***. Address specifying the customer interface of the Telenor CE router. This is next-hop IP address for the other VPN sites.

- ***Default Gateway***. Next-hop interface address for addresses that is not part of the customer VPN. Usually this is the Internet. May also be used for addresses in the VPN to avoid specifying every route in the VPN.
- ***LAN1 Next-Hop IP Address***. Describes the interface gateway address to another LAN that is to be reached from the customer CE router.
- ***LAN1 Address/LAN1 Mask***. Address and network specifying the address range of LAN1.

3.5.5 DHCP Relay

Mobile	Plus	Complete
Included	Included	Included

In addition to the option of using fixed IP addresses in the LAN connected to the access, the customer premises router also supports dynamic address allocation using DHCP.

The address allocation can be performed centrally from one or several customer-owned servers, which is common to the entire VPN. In this case the customer specifies one or several DHCP relays, also termed IP Helper Addresses, in order to point to the DHCP servers that distribute IP addresses.

3.5.6 DHCP Server in CE

Mobile	Plus	Complete
Included*)	Included*)	Not available

In addition to a centralized solution using DHCP relay, a DHCP server can be configured locally in the CE router.

The customer specifies an IP address for the CE router. The remaining IP addresses are distributed dynamically to the LAN hosts, except from addresses termed DHCP exclude, which act as fixed addresses for servers and printers e.g. Addresses can also be specified for Primary DNS and Secondary DNS.

Note:

*) DHCP server in CE for Managed Plus and Managed Mobile is not available in combination with the following optional service features:

- Multi-10
- Encryption

3.5.7 Customer Surveillance

Mobile	Plus	Complete
Included	Included	Included

Telenor is using SNMP access to the CE router for production of the statistics in WEBline for Nordic Connect. For those customers that wish to connect their own tool for management and statistics, Telenor can provide SNMP access to the CE router. Only one SNMP profile can be applied to a VPN. All sites in the VPN will be configured with the SNMP profile.

SNMP read parameters:

- SNMP read community. Only one SNMP read community per VPN
- SNMP read host. IP address for the servers or network that will have access to SNMP read on the CE router. Multiple hosts or networks allowed.
- SNMP trap host. IP address for the server that will receive SNMP traps from the CE router. Multiple hosts allowed.

SAA read/write: When using SAA read/write, the Customer should note that this could affect the capacity in the CE router and over the access.

- SNMP write community. Only one SNMP write community per VPN.
  Note: It has to be different from the SNMP read community
- SNMP write host. IP address for the servers or network that will have access to the SNMP SAA mib on the CE router. Multiple hosts or networks allowed.

3.5.8 Alerting for NC Managed Mobile

Alerting is a feature that must be activated by the customer via Webline.

If the CE router at a VPN site with NC Managed Mobile fails to respond for a period of 20 minutes, the customer will be alerted via e-mail and/or SMS that the site is down. After contacting Telenor and the fault has been corrected, the customer will receive another alert when the site is up and running again.

The recipients of alerts must be predefined by the customer in the contact information field in Webline.

3.6 Optional Service Features

Optional service features can be bought on demand to supplement the functionality of the standard service. Optional features will be charged with an OTC and a monthly fee. If the optional feature is installed as the main service is established, the OTC will be omitted.

3.6.1 Dynamic Routing LAN

Mobile	Plus	Complete
Not available	Optional*	Optional

Dynamic routing between the customer LAN and the network can be supplied as an option. Dynamic routing is implemented per VPN, which means that two VPN-accesses on the same access line can use different routing protocols.

Dynamic routing gives support to a large number of underlying subnets. Telenor support a maximum of 100 routes received from the customer LAN pr. VPN access and a maximum of 1000 per VPN. Exceptions from this rule must be discussed case by case.

Nordic Connect gives support for the following routing protocols:

- RIPv2
- OSPF v2 Area 0
- BGPv4

RIPv2 cannot be used as routing protocol on redundant solutions.

When BGP is selected as routing protocol, an AS number, a BGP peer IP address and an MD5 password must be supplied. The maximum length of the password is 15 characters, and the Nordic ASCII characters “æ, ø, å” and “space” are not valid.

Note:

*) Routing to default gateway (0-route) from Norwegian SHDSL access lines requires dynamic routing on the LAN interface.

3.6.2 Encryption

Mobile	Plus	Complete
Not available	Optional	Optional

Encryption is implemented as GET VPN with full mesh VPN topology. Maximum IP MTU size over an encrypted connection is 1378. Encryption/Decryption is performed in CE hardware.

Encryption algorithm is AES with 256 bit key length and SHA-1 hash algorithm.

Encryption can be implemented per VPN-access. All traffic across the VPN-access is encrypted.

Encryption is offered for bandwidths 64k-1000M as a standard service.

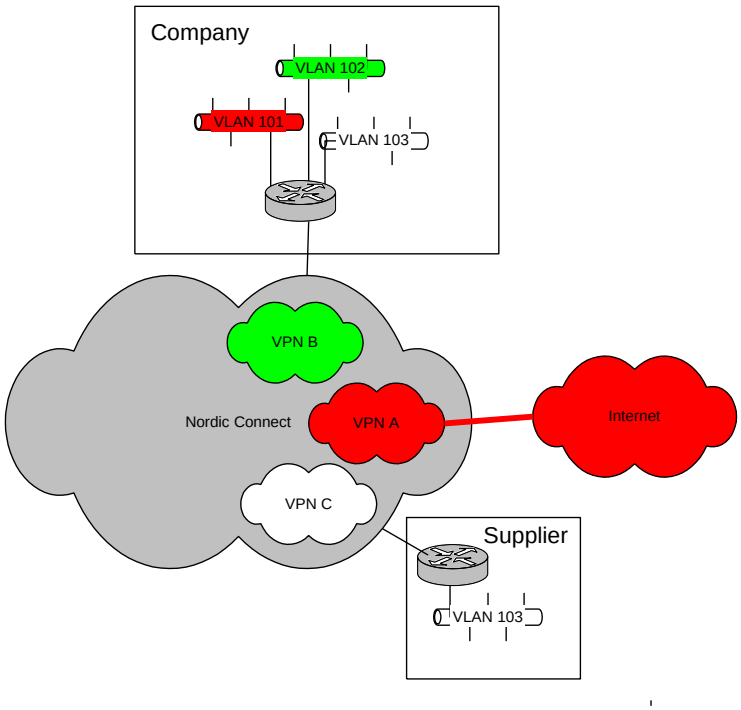
3.6.3 Support for additional VPNs

Service feature	Mobile	Plus	Complete
Multi VPN	Optional	Included	Included
Multi-10	Not Available	Optional	Optional
SP	Not Available	Not Available	Optional

The connection to one VPN is a standard service feature of every Nordic Connect access line. Connections to additional VPNs require support for one of the service features described in this section. On access lines with support for more than one VPN, the access to additional VPNs can be ordered as the optional add-on service *Extra VPN Access* described in section 3.6.4.

The figure below displays a customer with Multi-VPN. The interface supplied at the customer site is an 802.1Q trunk with three VLANs, each tagged with a unique 802.1Q-tag. The customer in the example has the following VPN structure:

- VLAN 101: VPN A (Internet)
- VLAN 102: VPN B (Company-internal)
- VLAN 103: VPN C (Supplier)



Figur 5 Example Multi-VPN solution

The total bandwidth on the access line is shared dynamically between traffic in all VPNs that use the access line. Functions such as traffic classification, routing and encryption are handled in parallel processes per VPN.

If the access line is part of a redundant solution, Telenor will reserve VLAN 17 for communication between the primary and secondary CE. This VLAN must be supported through the customers LAN infrastructure between the two CE routers.

3.6.3.1 Multi VPN

Mobile	Plus	Complete
Optional	Included	Included

For Nordic Connect Managed Plus and Complete, the included Multi VPN service feature supports connection to a maximum total of 5 VPNs over the same access line.

For Nordic Connect Managed Mobile, the optional Multi VPN add-on service supports connection to a maximum total of 3 VPNs over the same access line.

3.6.3.2 Multi-10

Mobile	Plus	Complete
Not available	Optional*	Optional

The option Multi-10 supports connection to a maximum total of 10 VPNs over the same access line.

*Except for Norwegian VDSL accesses, Multi-10 is only available for symmetric access types.

Notes:

1) In Sweden this option allows for a maximum connection of 8 VPNs over SHDSL access line.

3.6.3.3 Multi SP

Mobile	Plus	Complete
Not available	Not available	Optional

The option Multi SP supports connection to a maximum total of 50 VPNs over the same access line.

Multi SP will only be available for access speed ≥ 10 Mbps.

3.6.4 Extra VPN Access

Mobile	Plus	Complete
Optional	Optional	Optional

The option Extra VPN Access provides connection to an additional VPN over an access line.

The support for one of the service features described in 3.6.3 on the access line is a prerequisite for ordering this add-on service.

VPN-accesses are delivered as separate VLANs across an IEEE 802.1Q LAN interface. VLANs 100-909 are available for use by the customer. The customer should specify a VLAN id in this range as access to an additional VPN is ordered. It is recommended to use the same VLAN id on all access lines for a particular VPN.

3.6.5 Additional LAN-port

Mobile	Plus	Complete
Optional*	Optional*	Optional*

Additional delivery of extra physical LAN-ports is an option for Nordic Connect Managed. The number of LAN-ports that can be supplied for specific bandwidths and access technologies differ depending on the CE router in use.

Additional LAN-ports can only be supplied in conjunction with Multi-VPN. A LAN-port with Ethernet frames without VLAN tags can terminate one VPN. A LAN-port with VLAN tagged Ethernet frames (802.1Q) can terminate several VPNs. A particular VPN cannot be terminated on several LAN-ports.

The access bandwidth is shared between the LAN-ports.

Note:

*) The add-on service Multi VPN, Multi-10 or Multi SP is a prerequisite.

**) The CE used for Basic usually includes 4 switched Ethernet ports connected to a single VPN

3.6.6 QoS – Quality of Service

Add on service	Mobile	Plus [1)]	Complete
QoS 3 Classes (Q3C)	Not available	Optional	Optional
QoS 4 Classes (Q4C)	Not available	Optional	Optional
Custom QoS	Not available	Optional	Optional
Weight profile implementation	Optional [2)]		

Notes:
1) QoS is not supported for Basic and Plus in Sweden.
2) The implementation of minimum one customer specific weight profile is a prerequisite for ordering accesses with the Custom QoS model. The implementation is not associated with a specific access product.

Quality of Service (QoS) in Nordic Connect is based on the same approach as the DiffServ model described in RFC 2475. Service differentiation is achieved by categorizing traffic into different classes, and scheduling available resources in network elements between traffic aggregates based on QoS policies. This is in contrast to the IntServ approach described in RFC 1633, where signalling is used to reserve network resources before a session is started.

Three different QoS models with support for different number of traffic classes are supported:

- *QoS 4 Classes (Q4C)*
  It supports the following traffic classes:
  - 1 Expedited Forwarding (EF) traffic class.
  - 2 Assured Forwarding (AF) traffic classes.
  - 1 Default Forwarding (DF) traffic class.
- *QoS 3 Classes (Q3C)*

  It supports the following traffic classes:
  - 1 Expedited Forwarding (EF) traffic class.
  - 1 Assured Forwarding (AF) traffic class.
  - 1 Default Forwarding (DF) traffic class.
- *Custom QoS*
  The Custom QoS model is for customers with specific requirements that are not met by the Q4C model. It supports the following features:
  - 1 Expedited Forwarding (EF) traffic class.
  - 1, 2 or 3 Assured Forwarding (AF) QoS groups.
  - 1 Default Forwarding (DF) QoS group.
  - 1 or 2 levels of drop precedence within the AF and DF QoS groups, giving a possible total of 9 traffic classes (EF + 2*3*AF + 2*DF).
  - Customer specific weight profiles for allocation of bandwidth between the various AF and DF QoS groups.

3.6.6.1 Traffic classes

Characteristics for the various traffic classes are described below. In the Q4C and Q3C QoS models, the AF and DF QoS groups referred to in the description consist of one traffic class each. In the Custom QoS model, each of the AF and DF QoS group can consist of two traffic classes with different drop precedence.

- *EF – Expedited Forwarding*
  Traffic in the EF class is given strict priority on Nordic Connect access lines and through

Telenors MPLS core network. To avoid starvation of traffic in other classes, EF traffic is policed in CE and PE routers to a portion of the total access bandwidth.

- *AF – Assured Forwarding*
  Each AF QoS group is given a relative weight against other AF and DF QoS groups. If the access line becomes congested, each AF QoS group can utilize a ratio of the access bandwidth not used by the EF traffic class that corresponds to the relative weight of the AF QoS group. If there is no traffic in other traffic classes, traffic in each of the AF QoS groups may utilize the whole access bandwidth. Traffic in any of the AF QoS groups is given precedence over DF traffic through Telenors core network.
- *DF – Default Forwarding*
  Traffic not matched by any of the match criteria specified for other traffic classes belongs to the DF traffic class. The basic characteristic of the DF QoS group is the same as for the AF QoS groups. In the Q4C QoS model, the weight of the DF traffic class is smaller than the weight of each of the AF traffic classes.

The availability of traffic classes per QoS model is illustrated in Table 6.

Traffic class		**QoS model**		
QoS group	**QoS class**	**Q3C**	**Q4C**	**Custom**
EF	EF	X	X	x
AF4	AF4-LDP		X	x
	AF4-HDP			x
AF3	AF3-LDP	X	X	x
	AF3-HDP			x
AF2	AF2-LDP			x
	AF2-HDP			x
DF	DF	X	X	x
	DF-HDP			x

Table 6: Availabiliy of traffic classes per QoS model

LDP: Low Drop Precedence

HDP: High Drop Precedence

On accesses where differentiated drop precedence is introduced as part of the Custom QoS model, the probability of packet drop for traffic in a QoS group will increase with the utilization of that QoS group. Drop precedence is configured on WAN interfaces in CE and PE routers so that the drop probability for a HDP class will be 100% before drop probability for the corresponding LDP class increases due to traffic utilization.

3.6.6.2 Classification and marking

Classification is the process of detecting what QoS class traffic should belong to. This takes place in the CE router connected to the sender's LAN. The CE router will mark IP packets with traffic class by setting the value of the DSCP field in the IP header.

The policy for deciding which traffic class an application should use, and the criteria for how traffic belonging to a specific application is to be identified by a CE router, must be specified by the customer. Classification criteria are selected by choosing from pre-defined classification profiles. Each classification profile contains criteria for classifying traffic into one traffic class.

A set of globally available classification profiles that represent commonly used classification criteria can be selected by all Nordic Connect customers. In addition to this, customer specific classification profiles can be created according to criteria specified by a customer.

Match criteria for a classification profile can be defined using the following parameters:

- ***DSCP – DiffServ Code Point***
  IP packets with one or more DSCP values can be classified. The content of the DSCP field may be specified as IP precedence values instead of DSCP values for classification

purposes. To prevent remarking of the DSCP field by the Nordic Connect service, DSCP values used in the customers LAN should correspond to the marking described in Table 7.

- ***TCP/UDP-port number***
  If the involved applications or terminals are not capable of setting the DSCP/IP precedence bits in the IP header themselves, classification can be left to the CE router based on source or destination TCP/UDP-port numbers. Applications must use fixed port numbers or well-defined ranges of port numbers for this method of classification to work.

A classification profile can and should be associated with each of the EF and AF traffic class(es) that is going to be used on a VPN access. This may be done by defining a set of default classification profiles per VPN. The default classification profiles for a VPN will be applied to new accesses to the VPN unless they are overridden by classification profiles explicitly selected per VPN access.

IP packets that are not matched by any of the classification profiles associated with a VPN access will be marked as DF.

The use of the DSCP field for QoS marking by the Nordic Connect service is shown in Table 7.

QoS group	QoS class	DSCP value		
		Code point	Binary	Decimal
EF	EF	EF	101 110	46
AF4	AF4-HDP	AF43	100 110	38
	AF4-LDP	AF41	100 010	34
AF3	AF3-HDP	AF33	011 110	30
	AF3-LDP	AF31	011 010	26
AF2	AF2-HDP	AF23	010 110	22
	AF2-LDP	AF21	010 010	18
DF	DF-HDP		000 001	1
	DF	DF	000 000	0

Table 7: Traffic marking in the Nordic Connect service

The DSCP field will not be restored to its original value by the Nordic Connect service.

3.6.6.3 Weight profiles

A weight profile defines the relative weight of each AF and DF QoS group available on an access line.

For the Q3C and Q4C QoS models one of the available pre-defined weight profiles must be selected. The available weight profiles are shown in Table 8.

QoS group	Weight profile vs. QoS model[1)]				
	Q3C	Q4C			Custom
		Std-1	Std-2	Std-3	
EF[2)]	25%, 50%**Fejl! Henvisningskilde ikke fundet.**				
AF4		45%	60%	30%	[C4]
AF3	80%	45%	30%	60%	[C3]
AF2					[C2]
DF	20%	10%	10%	10%	[C1]

Table 8: Weight profiles for the Q4C and Q3C QoS models

The EF traffic class will be policed to either 25% or 50% of the access bandwidth, however maximum 500 Mbps of EF-traffic. CE and PE routers will discard EF traffic that exceeds this limit.

The access bandwidth not utilized by EF traffic will be scheduled between the AF and DF QoS groups according to the weight of each QoS group.

Note:

1) Ratios stated in Table 8 must be regarded as approximate values. Some deviation from these ratios must be expected during measurement.
2) The following restrictions apply to the EF traffic class:
   - For asymmetric accesses, the policed ratio for EF traffic relates to the minimum (i.e. upstream) bandwidth.
   - The EF traffic class is not supported on asymmetric accesses in Sweden.
   - In Norway, a minimum downlink bandwidth of 1 Mbit/s is required.

3.6.6.4 Technical service parameters

The Nordic Connect service offers SLA parameters for the following elements related to QoS:

- Delay
- Jitter
- Packet loss

Refer to section 4.2 for a description of values and conditions for these parameters.

3.6.7 Backup Access Lines

The following characteristics apply to a backup solution:

- The primary access line and the backup access line terminate in one CE router.
- The primary access line and the backup access line usually have different line speed.
- The backup access line utilizes an asymmetrical or symmetrical access technology.
- The customer can select which VPNs are to be rerouted to the backup service from the Primary. If backup filters are used (chapter 3.6.7.2), these must be defined per VPN.
- Traffic is automatically redirected to the backup access line if the primary access line is down. When the primary is available for traffic again, the traffic will automatically utilize the primary access line.
- There is no load-sharing between the primary access line and the backup access line. The backup access line will not carry traffic under normal operating conditions.
- This is an in-bound backup solution, as opposed to out-bound or around the cloud. Traffic to and from environments at the location connected over the Backup service will be transported in Nordic Connect core network, while communicating with its remote session peers.
- In a failover situation, where the backup is in operation and the primary access is down, the service will be considered available. Such situation will therefore not affect the guaranteed availability in the SLA and is not qualifying for any penalties.

3.6.7.1 Mobile Backup

Country	Plus			Complete	
	ADSL	SHDSL	VDSL	≤ 10M	> 10M
Norway	Optional	Optional		Optional	
Sweden	Optional			Optional	
Denmark	Optional		Optional	Optional	

Mobile backup is based on the mobile packet data network as access network as described in chapter 3.2.5. It is important to note that during a failover situation, the technical SLA for the primary access is not guaranteed. The main purpose with Mobile Backup therefore is to provide VPN sites with a backup

path for mission critical applications that do not require QoS while the primary service is being repaired. To ensure that only selected applications are allowed to use the backup line, customers can define an optional backup filter as described in chapter 3.6.7.2. The default is no filter.

Backup can be selected for a maximum of three VPN's. This limit is applicable even when the number of VPNs on the primary access is higher.

The following options to the main service are not supported in combination with mobile backup:

- Multi 10 and Multi SP
- Dynamic routing on LAN
- Hub-spoke topology

If the main service is Managed Plus or Complete (multi VPN), these limitations apply per VPN.

Maximum IP MTU size on the mobile backup line is 1476.

Mobile coverage on-site is the responsibility of the customer and must be acknowledged with customer during sales phase.

Mobile Backup availability is secured by proactive surveillance. Therefore it is mandatory to upgrade from the default SLA level included with the main product to either SLA level 4.7, 4.8 or 4.9.

3.6.7.2 Backup filter feature

Since available bandwidth on a backup line can be limited compared to the primary line, customers can define backup filter profiles that will allow only selected applications to use the backup line. The filter profile describes an access list (ACL) that will be provisioned on the CE router. Filter profiles can be specified for both directions if required:

- Outbound filter restricts traffic from the LAN towards the WAN-side
- Inbound filter restricts traffic from the WAN towards the LAN-side

Filter rules can be based on TCP/UDP port, port ranges, IP address or sub-networks. Furthermore they can be set for TCP/UDP ports only, IP addresses only, or in combination.

3.6.8 Redundant Access Lines

In a redundant solution the customer site is connected to Nordic Connect and Telenor's IP/MPLS-network via two access lines that terminate in two separate CE routers. The customer can select between two classes of redundancy:

Redundancy type	Physical redundancy	Possible SLA-levels
Active-passive with automatic failover (HSRP, BGP)	Full	SLA 6 [1)]
	Partly	SLA 5 og 5.3
Active-active with customer controlled loadsharing	Full	SLA 4 og 4.3 [2)]

1) A prerequisite for full redundancy is that the primary and secondary are of the same bandwidth.
2) Redundancy type active-active is not available in Sweden

3.6.8.1 Active-passive redundancy with automatic failover

In this solution one of the access lines is defined as primary (active) while the other is secondary (passive). HSRP signaling is used to control failover between the access lines and the two CE routers must be interconnected via an Ethernet LAN. VLAN 17 on LAN port 1 on the CE routers is designated for that purpose, and if necessary the customer is required to switch VLAN 17 traffic in the local network to ensure connectivity CE – CE.

During normal operation data traffic flows over the primary access line while the secondary is passive standby. When the primary fails traffic is rerouted and the secondary access becomes the active. BGP is the routing protocol that is deployed to control rerouting, and maximum rerouting time is 3 minutes. When the fault is corrected, the primary access again becomes active and traffic is re-routed once more.

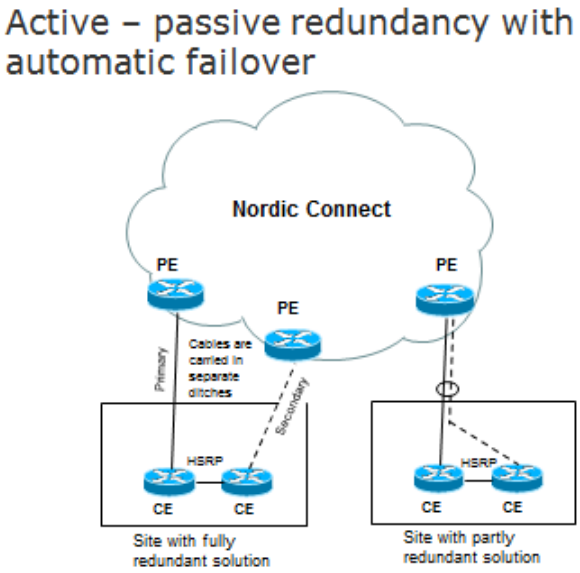


Figure 6 Redundant Solutions in Nordic Connect

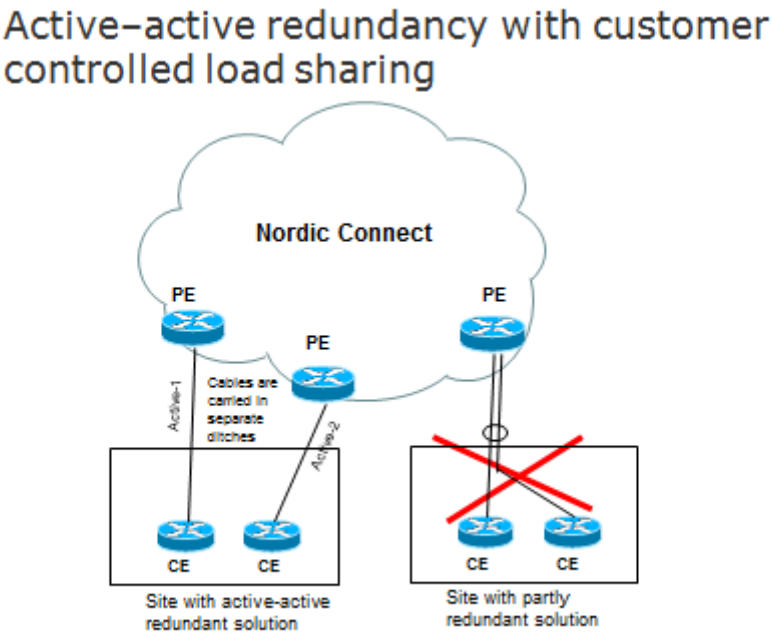
Fully redundant requires that the two access lines are carried in separate cables and ditches and are terminated in two geographically separate PE locations. Both access lines must be of type leased line and/or dark fiber with the same bandwidth. Fully redundant is a prerequisite to deliver SLA6 solutions, and one important benefit with SLA 6 is that Telenor will take these solutions into special consideration when planning for service and changes in the IP/MPLS network. Only one of the PE routers in a fully

redundant pair will be affected during the service window, and downtime will be limited to the failover time which is 3 minutes.

Partly redundant means the two access lines can have different bandwidth and that is possible to deploy other access types than leased line and dark fiber. This type of redundant solution is the basis for SLA 5 and SLA 5.3.

3.6.8.2 Active-active redundancy with customer controlled load sharing

This is a solution where the two Nordic Connect access lines are delivered in the same way as fully redundant active-passive solution. The difference is that there is no automatic failover mechanism provided as part of the service from Telenor. It is the customer who is responsible for how traffic are routed across the two access lines (load sharing), and this can be an attractive solution when failover is handled at the application level rather than the IP layer (BGP).



The difference between two regular NC Complete access lines and an active-active solution is that the access lines are provisioned as a *logical pair with cross-reference* (LU number). Therefore Telenor will treat active-active in the same way as SLA6 solutions, and only one of the PE routers in an active-active pair will be affected during planned work in the service window.

3.6.9 SHDSL Extra Wire Pairs

Plus	Complete
Optional*	Not available

Note: This add-on service applies to Norwegian SHDSL accesses only.

SHDSL accesses are by default delivered using the minimum number of wire pairs required for the selected access bandwidth, as specified by the G.SHDSL standard. Other combinations of wire pairs are supported on Norwegian SHDSL accesses as an optional add on service.

Additional wire pairs can be used to obtain SHDSL coverage in areas where SHDSL is otherwise not an available access technology. It can also be used to prepare for a future upgrade to an access bandwidth that requires a larger number of wire pairs.

The table below lists the numbers of wire pairs supported on the various SHDSL access bandwidths.

Access bandwidth	Number of wire pairs		
	1	2	4
0,5M SHDSL	Included	Not available	Not available
1M SHDSL	Included	Optional	Not available
2M SHDSL	Included	Optional	Optional
4M SHDSL	Not available	Included	Optional
8M SHDSL	Not available	Not available	Included

Table 9 Number of wire pairs vs SHDSL access bandwidth

4. SLA – Service Level Agreement

The document Nordic Connect Service Level Agreement (SLA document) is the master document for all SLA issues. If the content of this document differ from the SLA document, the SLA document is the legally binding document.

For descriptions of fault handling, planned works and customer service etc, see the SLA document.

4.1 Operational SLA

The Service window for Nordic Connect is Monday 01.00-06.00.

Access/site type	Monthly availability	Fix time		Automatic failover	Service time/SLA level		
		Physical [2]	Remote [3]		Mon – Fri [1] 0800 - 1700	Every day 0800 - 2200	Every day 0000 - 2400
Mobile	99,00 %	< 12h	< 12h	n/a	SLA 1	n/a	n/a
Managed Plus	99,50 %	< 12h (NO: < 8h)	< 4h	n/a	SLA 2	n/a	n/a
Managed Complete	99,60 %	< 8 h [4] (NO: < 5 h)	< 4 h	n/a	SLA 4	n/a	SLA 4.3 [5]
Backup	99,70 %	< 8 h (NO: < 5 h)	< 4 h	< 3 min	SLA 4.7	SLA 4.8 [5]	SLA 4.9 [5]
Redundant	99,80 %	< 8 h	< 4 h	< 3 min	n/a	SLA 5	SLA 5.3
Fully redundant	99,99 %	< 8 h	< 4 h	< 3 min	n/a	n/a	SLA 6

1) Normal working days
2) Norway/Denmark: Fix time includes time to restore redundant/secondary access.
   Sweden: Fix time for locations with backup or redundant access denotes time to restore main/primary access while traffic is running on redundant/secondary access.
3) Fix time, remote: Terminal based errors correction that does not involve hardware failure or errors in the access subnetwork.
4) Sweden: 12 hours physical error correction for accesses based on Skanova's Ethernet Sweden product (0800 – 1800, Monday – Friday only)
5) Availability of extended SLA levels depend on regional coverage, and must be verified for each site

Table 10 SLA levels in Nordic Connect

4.2 Technical service level

QoS group/ class	Parameter								
	Maximum			Condition set I			Condition set II		
	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss	Delay	Jitter	Packet loss
EF	100 ms	50 ms	0,01%	50 ms	25 ms	0,01%	25 ms	15 ms	0,01%
AF4	n/a	n/a	n/a	75 ms	40 ms	0,01%	50 ms	25 ms	0,01%
AF3	n/a	n/a	n/a	75 ms	40 ms	0,01%	50 ms	25 ms	0,01%
AF2	n/a	n/a	n/a	75 ms	40 ms	0,01%	50 ms	25 ms	0,01%
DF	n/a	n/a	n/a	100 ms	n/a	0,1%	75 ms	n/a	0,1%

Note:

- All values are one way from CE to CE and assume measurement of a 100-byte packet in IMIX (Internet mix) traffic.
- Packet loss for the EF QoS class is on condition that the traffic in the EF class is less than the policed rate for this class.
- Jitter values represent IPDV (Inter-Packet Delay Variation) standard deviation.
- All values for AF and DF QoS groups are on condition that traffic load for the QoS-group represents less than 75% of the weight for that QoS group.
- Jitter values for AF QoS groups only apply to QoS groups with a minimum weight of 60% on both access lines involved.
- Packet loss values do not apply to HDP QoS classes.

Condition set I:

- Minimum access bandwidth: 2M.
- Maximum distance between end points: 2000 km.

Condition set II:

- Minimum access bandwidth: 10M.
- Maximum distance between end points: 500 km.

5. Terms of delivery

5.1 Connection to Telenor's Network

It is Telenor's responsibility to terminate the access line at the first junction point, also termed the Point of connection. The customer must specify the location of the Point of connection, and is also responsible to ensure that Telenor and/or its contractors will be given access to the Point of connection during installation. The CPE delivered from Telenor should be positioned according to instruction from the customer; Point of delivery.

If the customer chooses different locations for point of connection and point of delivery, internal cabling will be necessary. This internal cabling is not part of the service, and can be provided for an additional fee.

The customer may select the specific cable to be used by Telenor at installation of the service. If the internal cabling fulfils Telenor's requirements, Telenor will finish installation of the service. If the customer does not select specific internal cabling, or if the internal cabling does not fulfil Telenor's requirements, internal cabling must be in place. The connection of the services must then be postponed until the internal cabling is installed.

Upon request, Telenor may commission an external contractor to fulfil the internal cabling. The fee for this is a separate agreement between the customer and the contractor.

5.2 Connection to Telenor's network with mobile access

A prerequisite for using these services is that the location of the CE-router at the customer premises is within coverage of the Telenor mobile network and has sufficient signal strength. It is the customer's responsibility to ensure that the preferred location of the CE (Point of Connection) is within mobile coverage. This is described in the attached installation instructions included with the router, as well as in Webline. As an option, Telenor can help the customer to check the mobile coverage and signal strength by doing a site survey (only available in Sweden). Telenor can also offer alternative antenna installations as an optional service.

5.3 Demands to Space where CE is installed

- The room must be no smaller than 1x1x1m.
- The CE must be placed in the customer premises.
- No intruders should have access to the premises.
- Telenor should have access to the premises for fault handling
- The premises should have ambient air temperature and relative humidity (23°C ± 5°C, 10-80% Relative humidity. Non-condensing temperature ranges).
- Failure tolerant power supply is recommended.

5.4 Local Area Network (LAN)

The customer is responsible for the LAN and all equipment connected to the LAN.

5.5 Control of Service Delivery

Installation of the service is always followed by a verification of service connectivity. If the service is installed by a Telenor technician this is a process between the technician and the Telenor operations center. If the service is installed by the customer this is a process between the customer and the Telenor operations center.

The test should verify IP connectivity between the CE and the service core network. If the test fails, troubleshooting will start according to contract.

5.6 Relocation of Service

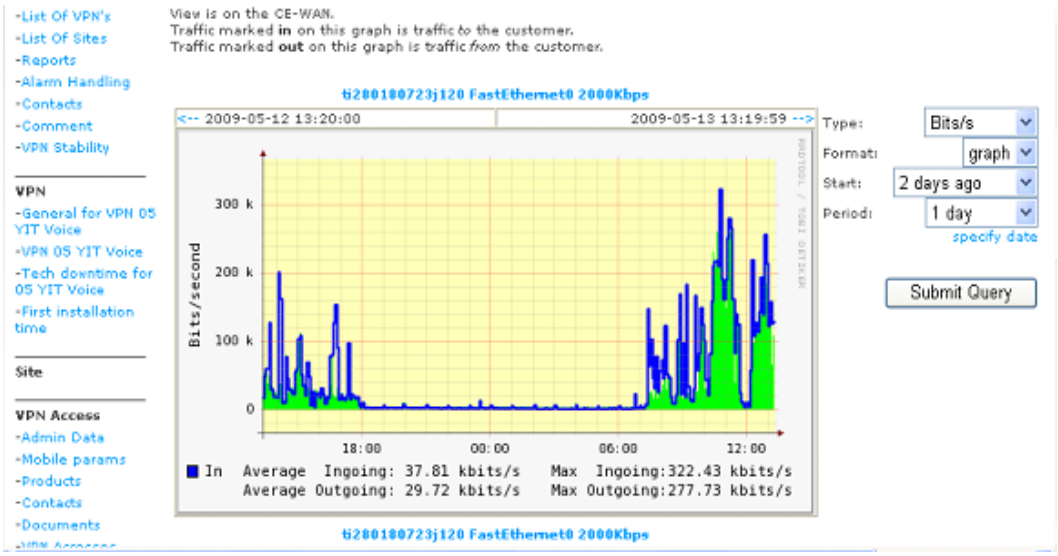
When the customer moves the service should be relocated. Relocation of the service will be charged as new business. The service can only be relocated to addresses where Telenor can deliver the service. Telenor will not perform a relocation of the service unless specified to do so by the customer.

6. Reporting

WEBline is included with the service Nordic Connect Managed. It is a tool for administration and statistics of the customer solution.

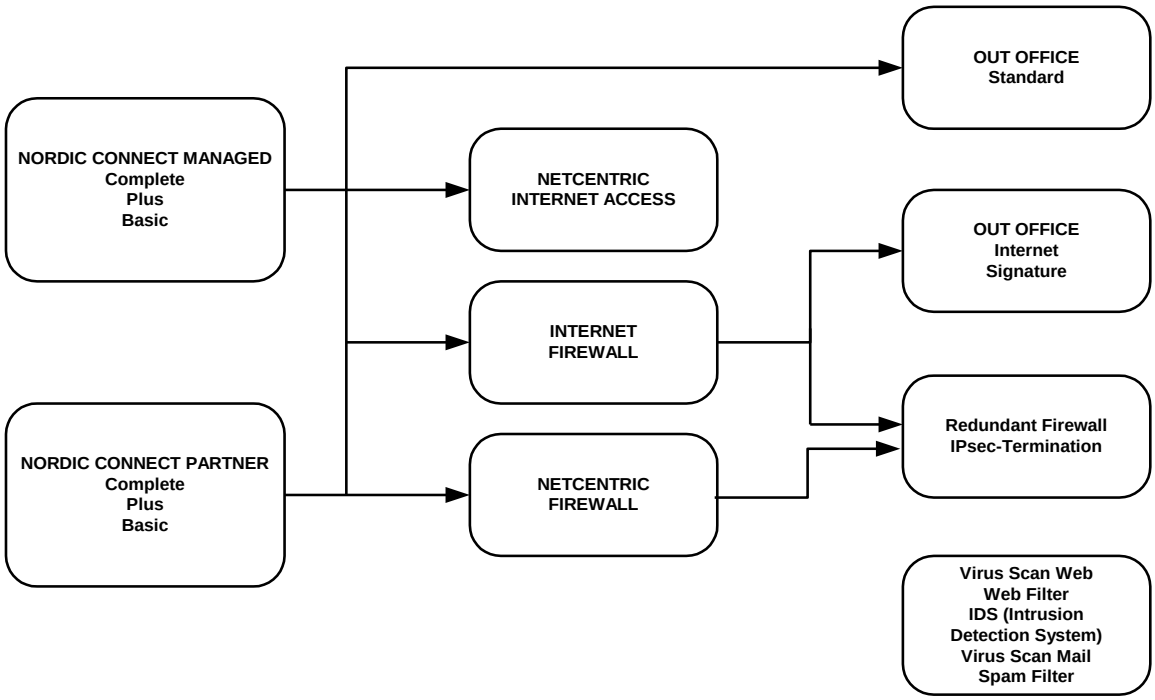
WEBline for Nordic Connect Managed includes the following services:

- An interface for administration and classification of WEBline users.
- Overview of the customer network solution
- Administrative view of each customer site
- Detailed technical parameters for each site
- Tables that displays technical availability and downtime
- Graphs showing total traffic, round-trip delay, jitter and packet-loss.
- A looking-glass function that provides access to certain functions in the customer located router, such as: ping, traceroute, show interface, show access-list etc.



Figur 7: Screen shot of WEBLine

7. Related Nordic Connect Products



Figur 8 Nordic Connect portfolio with related products

- ***NetCentric Firewall*** provides security between VPN's. The FW is placed net-centric for direct control of the flow of traffic between VPN's.
- ***Internet Firewall*** provides net-centric Internet access to the customer through a firewall managed by Telenor.
- ***NetCentric Internet Access*** provides net-centric Internet access to the customer. The solution does not include a firewall managed by Telenor, but leaves the customer to manage his own firewall solution.
- ***Virus Scan Web and Web Filter*** can be installed to provide better security against intrusion from the Internet.
- ***OutOffice Standard***: Dial-up single user access to a Nordic Connect VPN via PSTN, ISDN, ADSL (from Telenor), GSM or GPRS. At present OutOffice Standard is only available in Norway
- ***OutOffice Internet***: Location independent single user access to a Nordic Connect IP VPN through the Internet. Uses an encrypted tunnel from client software installed on the user's PC/PDA to a Nordic Connect Internet Firewall (IFW). Authenticated with user name and fixed password.
- ***OutOffice Signature***: Similar to OutOffice Internet, but with strong two-factor user authentication based on a fixed password combined with a one time password transmitted by SMS.
- ***Virus Scan Mail and Spam Filter*** can be installed to provide better security against intrusion from the Internet. ***At present Virus Scan Mail and Spam Filter are available only on request outside Norway.***
- ***Intrusion Detection Systems (IDS)*** can be implemented to provide surveillance, monitoring and analysis of the network 24x7x365. IDS will ensure the detection of any irregularities in the traffic pattern, and provides an effective protection against intrusion from the Internet. ***At present IDS is available only on request outside Norway.***

8. Document references

[1] Service Level Agreement for Nordic Connect.

[2] Service Description for OutOffice

[3] Service Description for Nordic Connect Security portfolio.

[4] User Manual for WEBline

[5] Service Description for Nordic Connect Partner

[6] Service Description for Nordic Connect Encryption

9. Terms and abbreviations

ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CE	Customer Edge
CPE	Customer Premises Equipment
HDP	High Drop Precedence
IP	Internet Protocol
IPDV	Inter Packet Delay Variation
ISP	Internet Service Provider
kbps	Kilobit(s) per second
LAN	Local Area Network
LDP	Low Drop Precedence
LL	Leased Line
Mbps	Megabit(s) per second
MPLS	Multi Protocol Label Switching
PE	Provider Edge
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RFC	Request for comment
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network