NODE4

Empowering business to do more

# Schedule document

## Secure SD WAN services

Public

Node4 Limited

*01/06/2024*

# Schedule document

## Secure SD-WAN Services

This schedule contains additional terms and conditions, service description and service levels applicable to the Secure SD-WAN Services and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

## 1. Overview

Node4 Secure SD-WAN Services provide the Client with a secure centrally managed software defined network, built on MPLS and Internet connectivity.

## 2. Definitions

***"Incident"*** *means* an unplanned interruption to a service or a reduction in service quality

***"Installation Fee"*** means charges payable by the Client for the installation of the service as provided in the Order Form;

***"Monthly Review Period"*** means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service performance measurements are calculated, provided that the first Monthly Review Period will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client;

***"Node4 Network"*** means the network wholly owned and managed by Node4;

***"Non-Service Affecting Incident"*** means an Incident or condition which is not a Service Affecting Incident.

***"Planned Outage"*** means proactive work required to maintain the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the outage with you in advance of the required work. Any planned downtime shall not be included in Incident or service reliability measurements;

***"Professional Service Fees"*** means the professional service charges detailed on the Order Form or otherwise agreed in writing between the Parties in accordance with Clause 4 below;

***"Service Affecting Incident"*** means any failure of Node4 service, which, in our reasonable opinion causes a loss of a Client's service. In all such cases the service shall be deemed unavailable and the length of downtime recorded by Node4 from when the Incident is registered by Node4 and a Service Ticket allocated.

***"Service Availability"*** means the time for which a Node4 service is usable, expressed as a percentage of the total time in a given Monthly Review Period. The Node4 service shall be deemed available for the purposes of calculating Service Availability if it is not usable due to an event outside our reasonable control, a Client Responsible Incident, a Third Party Attributable Incident or is due to a Planned Outage.

***"Service Desk"*** means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal.

**"Service Request"** means a request for a change for information

***"Service Ticket"*** means the tickets which are raised in relation to Incident or Service Request

**"Standard MAC"** means a change to one device which can be completed within 30 minutes by a support engineer between 7am and 7pm Monday to Friday.

## 3. Specific terms

The following terms and conditions shall apply when Node4 Connectivity Services to the Client.

**Multiple connections**
Where the Agreement comprises of a number of individual connectivity services, each will hold the Initial or Extended Term, starting upon activation of the particular service. If the Agreement is terminated by the Client while any of the individual connectivity services are still within their Initial or Extended Term, then the Node4 shall exercise right to levy appropriate Early Termination Charges as per

Clause 13.2 or the Terms and Conditions on a pro-rata basis, for outstanding rental charges on each of the individual connectivity services still within the Initial or Extended Term.

**Cancellation before implementation**
If the Client cancels the service prior to installation, but after the Supplier has committed to an agreed installation date, the Node4 reserves the right to pass on any costs reasonably incurred, including those incurred by the Third Party Services Provider. Where the service being cancelled is an Ethernet service, an additional administration fee of £350 will be levied.

**Third parties**
Node4 shall not be liable in respect of any contract, agreement or relationship that the Client may have with any third party. If a dispute arises between the Client and a third party involving Node4's MPLS services, Node4 shall provide the Client with reasonable information and assistance (to the extent that such is not adverse to Node4's interests to Client (at Client's expense) in the resolution of such dispute.

## 4. Fees

Installation and Rental Fees associated with each individual access component will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client, this will follow the installation of a specific connection.

**Reoccurring fees**
Rental Fees are paid monthly in advance based on the support provided and any other related service and are identified on the Order Form.

**Set-up fees**
Any applicable Design, Configuration, and Installation Fees for the implementation of the service shall be detailed on the Order Form.

Once an order is placed a survey is carried out which may identify excess construction charges, or other charges levied by 3rd parties such as legal fees to agree wayleaves. Any such Fees will be notified to the Client who may choose to accept them or cancel the order at no cost.

**Professional service fees**
Initial Professional service requirements will be stated on the Order Form

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

**Termination and change fees**
Node4 will notify the Client of any Additional Fees incurred from third parties resulting from changes or cancellations to the services provided, any additional fees will be included on the next invoice.

## 5. Client responsibilities

In order to deliver the service Node4 require the Client to provide or purchase from Node4:

- LAN IP Addressing & IP Routing information
- Assistance for the service provider when they visit the Client site (Abortive site visits are chargeable)
- Guiding the access network engineer to an agreed installation point at the Client site. Power, Ethernet port on LAN and suitable cabinet space for CPE
- The location of the circuit and the LAN port must be within 2metres of the router location.

## 6. Secure Bundles

The aspects and service components below together form the Node4 Secure SD – WAN Service offering. Please refer to your proposal or quote to understand what is included within your solution.

Secure bundles form the main service component for each location connected to the Secure SD-WAN. A bundle should be selected based on the site locations needs today and in the future.

**Secure DataCentre Bundle**
Each SD-WAN solution requires one Secure DataCentre bundle hosted within a Node4 DataCentre that includes:

- Dual Firewalls for High Availability
- Ethernet switches (2 per data centre)
- Tier 3 DataCentre Hosting
- A choice of Resilient Internet Breakout Speeds
- MPLS & Centralised Internet Breakout Ports
- Geo-resilience included in selected bundles
- A choice of managed service level
- Hardware + Software support
- Centralised Management + Reporting Portal
- Public IPv4 address allocation (quantity agreed per solution).
- Minimum 100MB of log file space per managed appliance or high-availability pair. (additional space is optionally available)

A choice of bundles available are shown in the below table:

| Bundle | Connection A | Connection B | Bandwidth Supported | Access Capacity | Geo-Resilient Deployment Across Two Node4 Facilities | Suitable for Virtualisation and Storage Networking | Suitable for Moderate Network Usage |
|---|---|---|---|---|---|---|---|
| **DC Bundle 1** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 10 Gbps | 84x 1/10GE Ports Per Data Centre | Yes | Yes | No |
| **DC Bundle 2** | **ConnectMPLS Private Access** | **ConnectFAST Internet Access** | **Up to 5 Gbps** | **84x 1/10GE Ports Per Data Centre** | **Yes** | **Yes** | **No** |
| **DC Bundle 3** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 1 Gbps | 38x 1/10GE Ports Per Data Centre | Yes | Yes | No |
| **DC Bundle 4** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 500 Mbps | 38x 1GE Ports Per Data Centre | Yes | No | Yes |
| **DC Bundle 5** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 100 Mbps | 38x 1GE Ports Per Data Centre | Yes | No | Yes |
| **DC Bundle 6** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 1 Gbps | 38x 1GE Ports Per Data Centre | No | Yes | No |
| **DC Bundle 7** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 500 Mbps | 38x 1GE Ports Per Data Centre | No | No | Yes |
| **DC Bundle 8** | ConnectMPLS Private Access | ConnectFAST Internet Access | Up to 100 Mbps | 38x 1GE Ports Per Data Centre | No | No | Yes |

**Secure Branch Bundle**

Each additional site that connects to the Secure SD-WAN requires a Secure Branch Bundle, the bundles should be selected from the below table based on connectivity type, level of resilience and bandwidth required. Each bundle will include:

- Firewall and Switch Hardware which is highly available where specified in the selected bundle.
- A choice of connectivity including Ethernet, xDSL and 4G.

A choice of bundles available are shown in the below table

| Bundle | Connection A | Connection B | Bandwidth Supported | Users Supported | Suitable for Business-Critical Locations | Suitable for Non-Critical Locations | Suitable for Heavy Voice, Video, Real-time or Cloud | Suitable for General Business Network Usage | Suitable for Light Business Network Usage | Suitable for Pop-up or Temporary Locations |
|---|---|---|---|---|---|---|---|---|---|---|
| BR1 | Ethernet | Ethernet | Up to 1 Gbps | 150 - 499 | Yes | No | Yes | No | No | No |
| BR2 | Ethernet | Ethernet | Up to 500 Mbps | 50 - 149 | Yes | No | Yes | No | No | No |
| BR3 | Ethernet | Ethernet | Up to 100 Mbps | 10 - 49 | Yes | No | Yes | No | No | No |
| BR4 | Ethernet | EoFTTC or FTTC | Up to 500 Mbps | 150 - 499 | Yes | No | No | Yes | No | No |
| BR5 | Ethernet | EoFTTC or FTTC | Up to 100 Mbps | 50 - 149 | Yes | No | No | Yes | No | No |
| BR6 | EoFTTC or FTTC | EoFTTC or FTTC | Up to 160 Mbps | 10 - 49 | Yes | No | No | Yes | No | No |
| BR7 | Ethernet | EoFTTC or FTTC | Up to 500 Mbps | 100 - 499 | No | Yes | No | Yes | No | No |
| BR8 | Ethernet | EoFTTC or FTTC | Up to 180 Mbps | 50 - 99 | No | Yes | No | Yes | No | No |
| BR9 | EoFTTC or FTTC | EoFTTC or FTTC | Up to 160 Mbps | 10 - 49 | No | Yes | No | Yes | No | No |
| BR10 | Ethernet | None | Up to 100 Mbos | 10 - 49 | No | Yes | No | No | Yes | No |
| BR11 | EoFTTC or FTTC | None | Up to 80 Mbps | 1 - 24 | No | Yes | No | No | Yes | No |
| BR12 | 4G | None | Up to 80 Mbps | 1 - 9 | No | Yes | No | No | No | Yes |

## 7. Standard services

The following aspects are included as standard in the service.

**Highly Available Firewalls**
Where this is specified in a bundle it provides a pair of secure next generation firewalls configured as a resilient solution. Where one device fails the other will take over the provision of connectivity services with minimal disruption. Stateful failover where implemented is expected to occur within 3 seconds, application and service recovery times are dependent on external factors.

**Geo Resilient Secure DataCentre Bundles**
Where specified on the selected bundle a pair of firewall appliances will be geo-located across two Node4 data centre facilities in a highly available configuration, to provide geographic resilience for internet breakout services and connection to MPLS network.

Stateful failover where implemented is expected to occur within 3 seconds, application and service recovery times are dependent on external factors.

**Software Upgrades**
Up to 2 bulk software upgrades are included as part of the service per year, to provide new features or maintain vendor support, across all managed devices. If these are not used within the year, they will not rollover to further years.

Where a security vulnerability or software issue threatens the integrity or availability of the network, Node4 will endeavour to upgrade in a mutually agreeable timeframe, additional to the standard inclusive upgrades. Unless Node4's SOC service is included, Node4 will not actively assess software vulnerabilities or monitor security events.

**Network Monitoring**
All managed devices will be monitored using SNMP on Node4's standard monitoring platform. Access to monitoring data can be made available through a web portal. Additional event alerting will be setup using FortiAnalyzer. Infrastructure related events will be sent to Node4's Service Desk where they will be handled in line with the standard support agreement. Node4 will not monitor security events as standard.

**Application Optimisation**
Where specified, in line with the Statement of Works document, application optimisation will be configured to prioritise specific application traffic and optimise bandwidth consumption. Standard Setup includes optimisation configuration for up to 10 applications or groups across up to 5 different branch bundle types.

**SaaS Application Traffic**
Where a Secure Branch bundle is ordered that has both MPLS and Direct Internet connectivity a centralised policy can be configured to route Cloud application traffic such as Office365 or Salesforce directly to the internet. Standard Setup includes policy control for up to 10 applications or groups across up to 5 different branch bundle types.

**Centralised Policy Management**
Standard setup allows for the configuration of 25 policies across up to 5 different branch bundle types within the centralised management portal and an agreed change process to push policy changes to Secure Branch devices.

**Monthly Reporting**
Standard setup includes the configuration of the Secure SD-WAN monthly report. This is a high level network traffic report that includes charts on traffic levels, application usage and detected security events. Amendments to this report are optionally available at additional cost. Clients can also develop their own reports free of charge where co-management arrangements have been agreed.

**Hardware and Software**
Node4 will provide management services for all provided network hardware and software. All hardware and software must have valid vendor support contracts.

Hardware maintenance is included with a valid vendor support contract, providing replacement hardware in the event of a vendor confirmed failure within 1 business day. As standard, Node4 will arrange for replacement hardware to be delivered direct to Client site and provide remote support (From Node4 Location) for the replacement activity. The Client is expected to provide remote hands and eyes, access to a computer on site with a console connection to the devices. Same day services and/or on-site engineer is optionally available at additional cost.

**Client support**
Node4 provides the service direct to the Client. The Client commits to fully manage all their customers and suppliers directly. Node4 will not interface directly with any third parties working with the Client. If the Client requires Node4 to provide their customers with a customer care or NOC service this is available on request and subject to Professional Service Fees.

**Maintenance window**
Where Node4 plans to perform essential works Node4 will endeavour to perform such works during low traffic periods and will endeavour to give the Client at least five (5) days prior notice. In the event of an emergency or Service affecting fault such notice may be less than 24 hours.

**Professional services**
Node4 can provide a full range of Support & Professional Services including but not limited to:

- On-site installation of routers & firewalls
- Remote support services including:
    - Network, router and firewall management
    - Monitoring and reporting
    - Network engineering and Design
    - Project Management
    - pre-configuration of routers and firewalls (this means that the router is pre-configured at Node4 and delivered to the Client site. The Client will have to provide someone on-site to connect the router)

Support on configuration is provided within business hours only and for a period not exceeding 15 working days from installation. Technical support is provided for the configuration implemented by Node4; we will not provide support for configuration outside of the original Client requirement.

The Professional Services are subject the Professional Service Fees. Specific rates for large or repeat orders can be agreed on a case by case basis in writing.

All incremental expenses incurred during these Professional Services will be passed directly to the Client. Provisioning costs such as cabling will be discussed and agreed with the Client in the Order Form.

**Changes**
Moves, Adds & Changes (MAC) are not provided as part of the standard service. If “Full Management” is included on the Order Form Standard MACs are included (fair use policy applies).

Change requests conducted outside of standard MACs, or support contract, or change request implemented outside normal business hours will be dealt with as chargeable projects and subject to the Support and Professional Services Fees in 4.3.

## 8. Managed Service

The following service options are available

**Fully Managed**
Fully Managed Service includes infrastructure Device Base Configuration, SD-WAN & UTM Configuration and Changes

**Co-Managed**
Co-Managed service includes Infrastructure Device Base Configuration Standard & complex changes

To qualify for this option the End user must have a network technical support team with 8 x 5 support

**Managed service options**
The table below provides the different managed service options available.

| | | Co-Managed | Fully Managed Service |
|---|---|---|---|
| **1st Line Support** | Priority 4 - 5 Support<br>Support for all services: Faults & all changes | | Included |
| **2nd Line Support** | P3 Support<br>Co-Managed Support | Included | Included |
| **3rd Line Support** | P1 & P2 Support<br>Infrastructure support, and fault escalation to 3rd line (NSE-4 or higher or equivilent) engineer | Included | Included |
| **Remote Break/Fix Support** | Node4 support service | Gold included | Gold included |
| **Remote Break/Fix Support -TAC** | Escalation to vendor TAC and management of TAC cases | Included | Included |
| **Moves, Adds, Changes** | If “Full Management” is included on the Order Form Node4 will provide standard moves, adds & changes services Standard MACs are included (fair use policy applies). Change requests are submitted through the Client portal on Service NOW | "Included: Operational management nt of the device and underlying network connectivity.<br>“Co-managed” with Client providing:<br>o 1st line support with escalation to Node4<br>o Standard changes to SD-WAN traffic polices<br>o Standard changes to next-generation features<br>" | "Included:<br>""Fully Managed""<br>Operational management of the device, underlying network connectivity and all features" |
| **Moves, Adds, Changes** | Limited patch management - Device is kept within vendor supported software version (upgrades performed with Node4 standard change control window 7am-7pm Mon-Fri excluding national holidays) – annual check and upgrade if necessary | Included | Included |
| **Standard Monitoring** | Standard Monitoring:<br>• Device availability – ICMP Ping & SNMP<br>• CPU Load<br>• Memory utilisation<br>• Temperature<br>• Interface status, Duplex error, L2 errors & utilisation<br>• Connections per second<br>• HA State | Included | Included |
| **Configuration Archiving** | Automatic configuration archiving via FortiManager | Included | Included |
| **Patch Management** | o Bi-yearly upgrades to the latest recommended software release (upgrades performed with Node4 standard change control window 7am-7pm Mon-Fri excluding national holidays) | | Included |
| **Patch Management - Well known vulnerability or OS issue likely to cause service impact** | o Upgrades to the latest recommended software release (upgrades performed with Node4 standard change control window 7am-7pm Mon-Fri excluding national holidays), no SLA | | Included |
| **On site Support** | Node4 On-site support service<br>Remote hands and eyes | Optional | Optional |
| **1st Line Support** | Priority 4 - 5 Support<br>Support for all services: Faults & all changes | | Included |
| **2nd Line Support** | P3 Support<br>Co-Managed Support | Included | Included |

## In addition to the above the following apply specifically to Dedicated FortiManager and FortiAnalyser

| | | Co-Managed | Fully Managed Service |
|---|---|---|---|
| **Standard Monitoring** | "Standard Monitoring:<br>• Device availability – ICMP Ping & HTTP<br>• CPU Load<br>• Memory utilisation<br>• Disk Usage" | Included | Included |
| **VM Backups** | VM Level-4 Management | Included | Included |
| **Patch Management** | Bi-yearly upgrades to the latest recommended software release (upgrades performed with Node4 standard change control window 7am-7pm Mon-Fri excluding national holidays) | Included | Included |

## 9. Site Connectivity

Bandwidth availability is dependent upon multiple factors such as the distance of the Client's premises from the exchange (EFM) or the Green Cabinet (EoFTTC, FTTC, Broadband and Mobile (3/4G)), bearer size and committed data rate (Fibre Leased Line) and the class of service applied to the circuit.

The Services can only be supplied within the available footprint and therefore some locations may not be eligible.

The following tables represents the different options which will be provided if included on the Order Form

### Mobile connectivity

| Product name | M2M – Machine to Machine |
|---|---|
| Alternative | 3G/46 |
| Available As | ConnextFast |
| Download Speed | N/A |
| Upload Speed | N/A |
| Product variants (Mbps) | 3G/4G |
| Access Presentation<br>Not router | Micro-SIM type 3F |
| Node4 Interconnect resilience | N/A |
| Service Contention | Standard |

### Broadband Products - Contended with extended repair times

| Product name | Broadband | Fibre Broadband | Fibre Broadband |
|---|---|---|---|
| Alternative | ADSL | FTTC Superfast Broadband | FTTP Superfast Broadband |
| Available As | ConnectFAST<br>Or<br>ConnectMPLS | | |
| Download Speed | Up to 24Mbps | Up to 80 Mbps | Up to 330 Mbps |
| Upload Speed | Up to 1.3Mbps | Up to 24Mbps | Up to 50 Mbps |
| Product variants (Mbps) | N/A | FTTC 80 (80:20)<br>FTTC 40 (40:10) | N/A |
| Access Presentation Not router | Uses WLR/PSTN Telephone line (NTE5/RJ11) Requires Microfilter | Uses WLR/PSTN Telephone line (NTE5/RJ11) Requires Microfilter | 1000BaseT |
| Node4 Interconnect resilience | Automated Geo Diverse failover | Automated Geo Diverse failover | Automated Geo Diverse failover |
| Service Contention | Standard Elevated traffic available | Standard Elevated traffic available | Standard |

### Ethernet Products- Uncontended with fast repair times

| Product name | Ethernet over FTTC | Ethernet First Mile | Fibre Leased Line | Wireless Leased Line |
|---|---|---|---|---|
| Alternative | EoFTTC /GEA | EFM | Ethernet | Ethernet |
| Available as | ConnectFAST, ConnectMPLS<br>Or<br>Point to Point | | | |
| Download Speed | Up to 20Mbps Burstable to 80Mbps | Up to 35Mbps | From 10Mb - 10Gb | From 10Mb - 1Gb |
| Upload Speed | Up to 15Mbps Burstable to 20Mbps | Up to 35Mbps | From 10-10Gb | From 10-1Gb |
| Product variants (Mbps) | Uncapped (80:20) Fixed (20:20 or 3:3) | 1-8 Pairs (Each pair effects the speed) | 10-10Gb | 10-1Gb |
| Access Presentation Not router | 100BASET or NTE5/RJ11 | 10BASET or 100BASET | 100Mb: 100BASET or<br>1Gb: 1000BASESX(orLX) 1000BASET May be available on require | 1000Base-T |
| Node4 Interconnect resilience | Not automated - Please design if required | Not automated - Please design if required | Not automated - Please design if required | Not automated - Please design if required |
| Service Contention | Low Guaranteed to the upload | Low Guaranteed minimum | No | No |

### Core network utilisation

The below defines how each variation of connectivity effects the core network utilisation of the product.

connectfast: The Node4 ConnectFast service utilises the Node4 Core Network to connect the Service directly to the public internet. As standard a Single Public IPv4 will be issued.

connectmpls: The Node4 ConnectMPLS service utilises the Node4 Core Network to connect the Service to a dedicated L3VPN MPLS or VPLS. As standard, private IPv4 addresses will be issued. (ConnectMPLS services do not provide access to the internet as standard. Central Internet Breakout services are available as part of the data centre bundle options).

### IP addressing and routing protocols

Node4 can provide SD WAN Clients with public internet access through ConnectFAST or Central Internet Breakout. All internet usage is subject to the Acceptable Use Policy (AUP)

For ConnectMPLS, Node4 will allocate IP address for internal routing that will be confirmed as usable with the Client.

For secure branch deployments, the Client must provide documentation clearly identifying what IP addressing will be used on Client LAN interfaces. Dynamic BGP routing or static routes can be configured towards Client branch equipment if required.

The number of public IPv4 addresses assigned will identified on the Order Form. Additional public IPv4 addresses can be rented from Node4. It is the Client’s responsibility to use their assigned IP addresses. Use of non-assigned IP addresses will result in immediate disconnection from the network.

Public IPv6 is also available if required, at additional cost.

**Bring Your Own Network**

In some cases, Node4 will allow 3rd party connectivity to be used with our SD-WAN solution. This must be standards based internet connectivity, such as national Ethernet, xDSL or 4G. In all cases Node4 must approve the use of this connectivity. Node4 will not provide support or service level assurances where 3rd party connectivity is used. All responsibility for 3rd party connectivity remains with the Client.

# 10. Asset management

## 10.1 General

If defined on the Order Form Node4 asset management service captures and updates key information about managed devices into a CMDB portal, assigns a unique asset number from the service tag and provides reporting via a Client accessible online portal and as part of the existing scheduled service reviews.

## 10.2 Asset entity definition and data

Assets which can be included are assets that can have an agent installed / respond to polling (switch, router, firewall etc) - Data is updated at point the agent is polled or checks in, most recent data is therefore at the point the devices was last seen online. The following online assets can be included

- Router
- DSL modem
- Switch
- Firewall
- Wireless Access Point
- GSM/LTE Modem (USB)
- SIM Card
- UPS (with ethernet management interface)

For these assets, the following information will be captured

| Asset data fields |
|---|
| Date Purchased |
| Vendor Serial # |
| Warranty or Support Subscription |
| Warranty or Support Expiry |
| Asset Tag (Physical) |
| Client Acc # |
| Registered User / Stock Location |
| Previous Registered Users |
| User Profiles Present |
| Accountable Manager |
| Last Audited Date |
| Registered Location of Asset |
| Installed Operating System |
| Patch Status |
| Last Seen - When |
| Last Seen - Where |
| Repair History |
| Parent/Child Relationships |
| MAC Address |
| Device Name |

## 10.3 Asset tags

If defined on the Order Form Node4 will provide tamper proof asset management stickers which include a barcode and unique identifier.

A service for applying the tags to devices is available on request at an additional cost.

## 10.4 Reporting

Reports will be included in any existing scheduled service reviews.

A portal is provided with read only access for the Client with the ability to produce summary reports of the assets being managed. Access to the portal is optionally secured using Single Sign On (SSO) authentication, (SSO service available separately).

## 10.5 Online asset service dependencies

The asset management services are depended upon the use of the tools provided by Node4.

# 11. Incident management

**Incident handling**

Incidents are handled as outlined in the Incident Management Schedule Document.

### Hours of support

The following table details the different Support Hours relating to the support hours defined on the Order Form.

| Support Hours | |
|---|---|
| Bronze | Standard business hours support 9am to 5.30pm week days, excluding bank and national holidays |
| Silver | Support hours between 7am and 7pm weekdays, excluding bank and national holidays |
| Silver Plus | Priority 1 and 2 - Support hours between 7am and 7pm 7-days a week, including bank and national holidays, excluding Christmas day, Boxing day and new year's day<br>Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays |
| Gold | Priority 1 and 2 - Support hours 24/7<br>Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays |

### Incident priority

Each new Incident will be assigned a priority level by the Service Desk based on the following definitions. These levels allow us to prioritise resources and escalate where appropriate.

| Priority | Description |
|---|---|
| 1 - Critical | A major Incident resulting in total loss of service. |
| 2 - High | A major Incident resulting in a severe service degradation or loss of service to a significant percentage of users. |
| 3 - Medium | A minor Incident resulting in a limited or degraded service or a single end user unable to work. |
| 4 - Low | General, single user with degraded service, non-service affecting support. |
| 5 - Service Request | Request for a change to an existing service or system, a request for information or simple questionnaire to be completed. |

### Incident duration

All Incidents recorded by the network management system will be reconciled against the corresponding Service Ticket raised by the Service Desk.

The exact Incident duration will be calculated as the elapsed time between the Service Ticket being opened and the time when Service is restored.

### Time to repair

Node4 aims to resolve Incidents in relation to the Connectivity services within the following times:

| Priority | P1 | P2 | P3 | P4 | Service Request |
|---|---|---|---|---|---|
| Response / Acknowledgement | 30 Mins | 1 Hour | 2 Hours | 4 Hours | 12 Hours |
| Commencement | 1 Hour | 2 Hours | 4 Hours | N/A | N/A |
| Frequency of Updates | 1 Hour | 2 Hours | 12 hours if Resolve / Target to Fix exceeded | | |
| Resolve / Target to Fix Ethernet | 5 Hours | 8 Hours | 12 Hours | 36 Hours | 60 Hours |
| Resolve / Target to Fix EFM and EoFTTC | 7 Hours | 12 Hours | 24 Hours | 60 Hours | 60 Hours |
| Resolve / Target to Fix FTTC, Broadband and Mobile | 24 Hours | 36 Hours | 48 Hours | 60 Hours | 60 Hours |

Resolution times in the table above do not apply where there is a Client Responsible Incident, a Third Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All priority 1 & 2 Incidents should be raised via the Service Desk system by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Client is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

***Where Incident resolution involves third parties, or hardware replacement, then this is subject to the support contracts in place with those parties.***

## 12. Service Level Agreement

### Service credits

Node4 will provide the Client with Service Credits, as set out below, for the failure to meet the following targets:

### Service availability

The Service is “Available” when the Client connection is authenticated and the Client can send and receive IP traffic.

The following equation will be used to calculate Service Availability. References to minutes are to the number of minutes in the applicable Monthly Review Period:

((Total minutes – Total minutes Unavailable)/ Total minutes) x 100

Credits for outages will be calculated on a monthly basis and will be based upon the cumulative elapsed time of any outages and the monthly Fee for the Service for each Client Site.

Node4’s goal is to achieve the Service availability per month for each Connectivity Service as defined in the table below;

| Service Credits (percentage) of monthly recurring Fees for the SD WAN Service at the relevant (Client Site) | Total monthly Availbility at the relevant Client Site (Percentage) | |
|---|---|---|
| | Ethernet over FTTC<br>Ethernet First Mile<br>Fibre Leased Line | Broadband<br>Fibre Broadband |
| 0% | 99.90% and above | 99.50% and above |
| 5% | <99.90% – 99.5% | <99.5% - 99.0% |
| 10% | <99.5% - 99.0% | <99.0% - 98.5% |
| 20% | <99.0% | < 98.5% |

### Calculation of services credits

Where a Monthly Review Period incorporates part of a month, any Service credit will apply to a pro-rated Monthly Fee.

Service credits will be calculated monthly, aggregated and credited to the Client on a quarterly basis.

If a Service is cancelled during a Monthly Review Period, no Service credit will be payable in respect of that Circuit for that Monthly Review Period.

The Client must claim any Service credit due to a failure to meet the Service levels, in writing, within twenty one (21) business days of the date at which the Client could reasonably be expected to become aware of such failure. The Client shall not be entitled to any Service credits in respect of a claim unless and until Node4 has received notice of the claim in writing in accordance with the above. Should Node4 require additional information from the Client, the Client shall assist, and shall not be entitled to any Service credits until Node4 has received all the information ir has reasonably requested.

### Exclusions of payment of service credits

Service credits will not be payable by Node4 to the Client in relation to the Service Availability for Incidents or disruptions to the Service caused by any of the following:

- The Incident, action or negligence of the Client, its employees, agents or contractors;
- The Client failing to comply with Node4’s Standard Terms and Conditions;
- An Incident , or any other problem associated with, equipment connected on the Client’s side of the Node4 Network Termination Point, except where such Incident or problem is directly caused by the action or negligence of Node4, its employees, agents or contractors;
- Any event described in Clause 10 (Force Majeure) of Node4’s Standard Terms and Conditions;
- A failure by the Client to give Node4 access to any equipment after being requested to do so by Node4; or
- Maintenance during any Planned Outage
- Where the Client is unable to provide 24 hour site access
- Broadband, FTTC and EoFTTC Incidents relating to the WLR line.
- Environment being outside of manufacturers operating guidelines for the equipment

Service credits are not applicable for more than one breach of any targets outlined in this document arising from the same occurrence.

The provision of Service credits shall be the sole and exclusive remedy for the failure to meet targets for the Connectivity service. Node4 shall have no additional liability to the Client.

# Appendix A

## 1. Core network statistics

### Class of service

### Transit delay

Transit Delay is a monthly measure of Node4's network-wide delay, which is the average interval of time it takes during the applicable calendar month for test packets of data to travel between all selected test pairs of Node4's MPLS PE Routers. Specifically, the time it takes test packets to travel from one MPLS PE router to another within our core network. Latency for the month is the average of all of these measurements.

### Delivery ratio

The "Delivery Ratio Percentage" for the core network is the average Data Delivery percentage for that month for all selected test pairs of Node4's MPLS PE routers calculated by dividing Data Received by Data Delivered and multiplying by 100. "Data Delivered" is the number of test packets of data delivered in a month by Node4 to from one MPLS PE router to another. "Data Received" is the number of such test packets of data that are actually received by the MPLS PE router. "Node4 MPLS PE routers" are the core MPLS routing nodes in the Node4's network consisting of Juniper MX series Ethernet routers.

### Jitter

"MPLS Jitter" is a monthly measure of the Node4 Network-wide IP packet delay variation within our core network, which is the average difference in the interval of time it takes during the applicable calendar month for selected pairs of test packets of data in data streams to travel between selected pairs of MPLS PE routers. Specifically, the difference in time it takes a selected pair of test packets in a data stream to travel from one MPLS PE router in a pair to another is measured for all selected pairs of MPLS PE routers over the month. One of the test packets in the selected pair will always be a packet in the data stream that takes the least time to travel from one Node4 MPLS PE router in the pair to another. MPLS Jitter for the month is the average of all of these measurements. "Node4 MPLS PE routers" are the core MPLS routing nodes in the Node4's Network consisting of Juniper MX series Ethernet routers.

The following table shows the target performance for ConnectMPLS and POP Interconnect Services:

| Description | BE | AF-HDP | AF-LDP | EF |
|---|---|---|---|---|
| Transit Delay | 40ms | 30ms | 20ms | 10ms |
| Delivery Ratio | 99.9% | 99.99% | 99.99% | 99.99% |
| Jitter | n/a | n/a | n/a | 8ms<br>(1-way) |

## 2. MPLS Options

### Class of Service

Four Client class of service categories are supported throughout Node4's core MPLS network. These being:

### Best effort (BE)

This class is the default class, all traffic not prioritized in the other queues will be serviced in this class. Typical traffic for this queue is web browsing, e-mail and FTP.

### Assured forwarding – High drop precedence (AF-HDP)

This class is the second class for data applications, e.g. ERP, database applications. Generally used for business critical applications, it provides guarantees of bandwidth. AF HDP traffic is prioritised above BE traffic. If/when congestion occurs BE traffic will be dropped in preference of AF traffic.

### Assured forwarding – Low Ddop precendence (AF-LDP)

This class is the highest class for data applications, e.g. ERP, financial transactions. Generally used for business critical applications, it provides guarantees of bandwidth. AF-LDP traffic is prioritised above AF HDP traffic. If/when congestion occurs BE then AF-HDP traffic will be dropped in preference of AF-LDP traffic.

### Expedited forwarding

This class is configured as a Priority Queue reserved for latency-sensitive applications only. The Priority Queue is guaranteed bandwidth based on the Client's bandwidth allocation. The priority command implements a maximum bandwidth guarantee. The priority queue is reserved only for Voice over IP (VoIP) or Video over IP traffic

Access circuits (Ethernet/DSL) may only support two or three classes of service – dependant on the service type.

## 3. Class of service options

ConnectMPLS L3VPN services being utilised for standard data services only will be assigned to the BE class of service. When used for site-to-site or multisite deployments by default will assigned to the BE class of service – the Client can request class of service be enabled.

The following profile options are application to ConnectMPLS:

| Profile | MPLS QoS Class | Bandwidth |
|---|---|---|
| 1 | BE / Default<br>AF | 50%<br>50% |
| 2 | BE / Default<br>EF | 50%<br>50% |
| 3 | AF | 100% |
| 4 | AF<br>EF | 50%<br>50% |
| 5 | EF | 100% |

POPI L2VPN services (Ethernet CCC or VLAN CCC) will be assigned to the AF LDP class of service.

## 4. Class mappings

For ConnectMPLS, Clients must pre-classify traffic using a DSCP value. We will honour these markings and associated the traffic to the appropriate queue.

The following table shows the standard DSCP to class mapping used within Node4's MPLS Network:

| DSCP | MPLS QoS Class | Application Use |
|---|---|---|
| 0 | BE / Default | Delay-tolerant Application – Email, Internet, FTP |
| 10,18 | AF-HDP | Mission Critical Application |
| 26,34 | AF-LDP | Mission Critical, Delay Sensitive Application, Real-time Multimedia |
| 46 | EF | VoIP, Unified Communications |
| 48 | NC | Routing Protocols |

## 5. Quality of service

QoS is provided end-to-end by using consistent DSCP and IP Prec values throughout the wide area and local area networks. We monitor network capacity to ensure that QoS is maintained.

The following table shows the QoS functions available for ConnectMPLS Services:

| Function | Description |
|---|---|
| Traffic Classification | DSCP, IP PRec – L3VPN<br>Interface or VLAN – L2 or L3VPN |
| Traffic Marking | DSCP<br>MPLS Experimental (EXP) |
| Congestion Management | Low Latency Queuing – L3VPN<br>Class-based weighted Queuing – L3VPN |
| Congestion Avoidance | Weighted Random Early Detection (WRED) – L3VPN |
| Traffic Conditioning | Shaping and Policing |