

ReSinc / HLB



Rede de Sincronismo
à
Hora Legal Brasileira

Manual Técnico

Outubro / 2006

Versão 3.0

1 - INTRODUÇÃO

Atualmente, a maioria das empresas utiliza redes de computadores. Evidentemente todos os computadores possuem relógios internos que deveriam funcionar sincronizados com a mesma hora.

A falta de sincronismo em seus computadores pode resultar em danos para a empresa, principalmente se a mesma realiza compras, vendas, aplicações financeiras e outras transações comerciais nas quais custos, lucros e multas estejam vinculadas ao parâmetro tempo.

Com o objetivo de prover um serviço de sincronismo confiável, rastreável aos padrões nacional e internacional (BIPM, Bureau International des Poids et Mesures) a Divisão Serviço da Hora (DSH) do Observatório Nacional (ON), montou a Rede de Sincronismo à Hora Legal Brasileira (ReSinc/HLB), para atender à órgãos públicos, empresas de quaisquer natureza e outros clientes que necessitem do tempo com exatidão.

A criação desta rede de sincronismo, não extingue os serviços fornecidos gratuitamente pela DSH, conforme descrito em nossa página <http://pcdsh01.on.br/SincPub.html> . Tais serviços estão com acesso liberado para todos, porem não são emitidos certificados para este serviço gratuito.

Para os participantes da ReSinc/HLB o ON emitirá mensalmente, certificado de que os respectivos equipamentos estiveram sincronizados no mês anterior. Tais certificados não se aplicarão a quaisquer usuários indiretos.

2 – SEGURANÇA DO SISTEMA

A ReSinc/HLB pode fornecer o sincronismo certificado de duas formas possíveis, por conexões utilizando linhas telefônicas e por conexões via Internet. Os sistemas adotados possuem dentre outras características, a capacidade de sincronizar *Mainframes* em salas cofres, com total segurança.

Caso se utilizem as linhas telefônicas é necessário o uso do protocolo o ACTS, desenvolvido pelo NIST (*National Institute os Standards and Technology*) (Michael A. Lombardi, "*Computer Timekeeping*", NIST, 1996). Tal procedimento garante o acesso à Hora Legal Brasileira com uma incerteza de ± 5 milissegundos no melhor caso possível.

Por intermédio de conexões via Internet é utilizado o protocolo NTP (Network Time Protocol), com os recursos de autenticação, chaves simétricas ou autochaves, ativados.

A falta de sincronismo, poderá ainda invalidar os arquivos de LOG:

a) Os carimbos de tempo (*time stamping*) , nos *log* de sistema. Estes são as evidências que se tem para tentar rastrear os caminhos percorridos pelos *hackers*, dentro do sistema invadido, possibilitando uma melhor prevenção de futuros ataques. Entretanto, se não houver sincronismo entre os diversos computadores ficará muito mais difícil seguir os passos do *hacker*.

b) Quando houver gargalos na rede, os registros de *log* poderão ajudar a solucionar o problema, pois estes *logs* consistem em carimbos de tempo a partir de diversas máquinas e, neste caso, o sincronismo terá uma grande importância na reconstrução da cronologia dos eventos.

3 - SOLUÇÃO ADOTADA

Com o intuito de prover maior segurança aos usuários, o sistema adotado pela ReSinc/HLB tem quatro premissas básicas, a saber:

1º : Os computadores não passarão pelo *firewall* da empresa e nem irão até o exterior para obter o sincronismo;

2º : Todos os relógios internos dos computadores serão sincronizados por um único servidor de tempo;

3º : A conexão do usuário com o ON será feita por uma linha telefônica comum ou por intermédio de conexões utilizando recursos de segurança baseados em SSH, SSL, SCP, STFT.

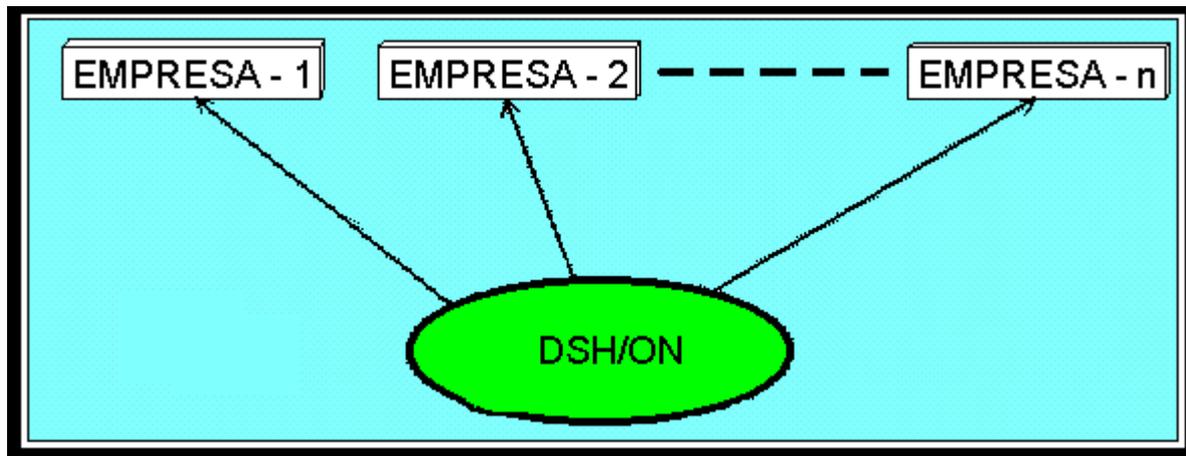
4º : O equipamento do cliente deverá se conectar ao ON periodicamente.

Os equipamentos pertencentes ao ON, Padrão Atômico de Césio, Gerador de Código IRIG, e os demais equipamentos sob a responsabilidade do ON, estão instalados em local com fornecimento de energia, refrigeração sem interrupção, 24 horas por dia, 7 dias por semana, 365 dias por ano, segurança, vigilância, proteção contra incêndio, raios, que asseguram autonomia de funcionamento.

O sistema é supervisionado remotamente, sem interferências no funcionamento normal.

3.1 - Arquitetura do Sistema

Cada empresa receberá o sinal de sincronismo diretamente da DSH do ON, garantindo-se desta forma uma única fonte de tempo.



3.2 - Detalhes da ligação ON ⇒ empresa

Conforme explicado no item 2, a conexão ao ON poderá ser feita por linha telefônica discada comum ou pela Internet. Se for por linha telefônica, a comunicação dar-se-á a cada 8 horas, garantindo-se um erro máximo menor que ± 5 milissegundos para o melhor caso possível, e de ± 80 milissegundos para o pior caso possível. O equipamento (NetClock 9283) sob a guarda do ON é idêntico ao que será instalado na empresa, mudando-se somente a sua configuração, o que fica no ON é configurado como servidor e o que fica no cliente é configurado como cliente. O equipamento sob a responsabilidade do ON, é sincronizado 5.000.000 de vezes por segundo por um relógio atômico, que por sua vez é rastreável ao UTC (*Coordinated Universal Time*), conforme explicado no item 4. As diversas saídas e entradas do equipamento que ficará nas empresas clientes são a seguir descritas. Estas ligações são registradas em arquivos de *log*, tanto no servidor quanto no cliente. Estes *logs* são acessados e analisados pelo ON, para posterior emissão de relatórios e certificados.

Sendo a conexão feita pela Internet é utilizado o protocolo NTP versão 4.2.0 com autenticação por chaves simétricas ou *autokey* (uma automatização do método das chaves simétricas). O NTP pode ser configurado para operar no modo *unicast* ou no modo *multicast* ou em ambos os modos. A capacidade de atendimento é de até 4000 sincronizações por segundo, no modo sem autenticação, e de 340 sincronizações por segundo no modo de autenticação. A utilização do modo de autenticação assegura que o equipamento instalado no cliente seja sincronizado pelo ON. Após o sincronismo inicial, o equipamento no lado do cliente passará a ser sincronizado a cada 17 minutos pelo equipamento no lado do ON.

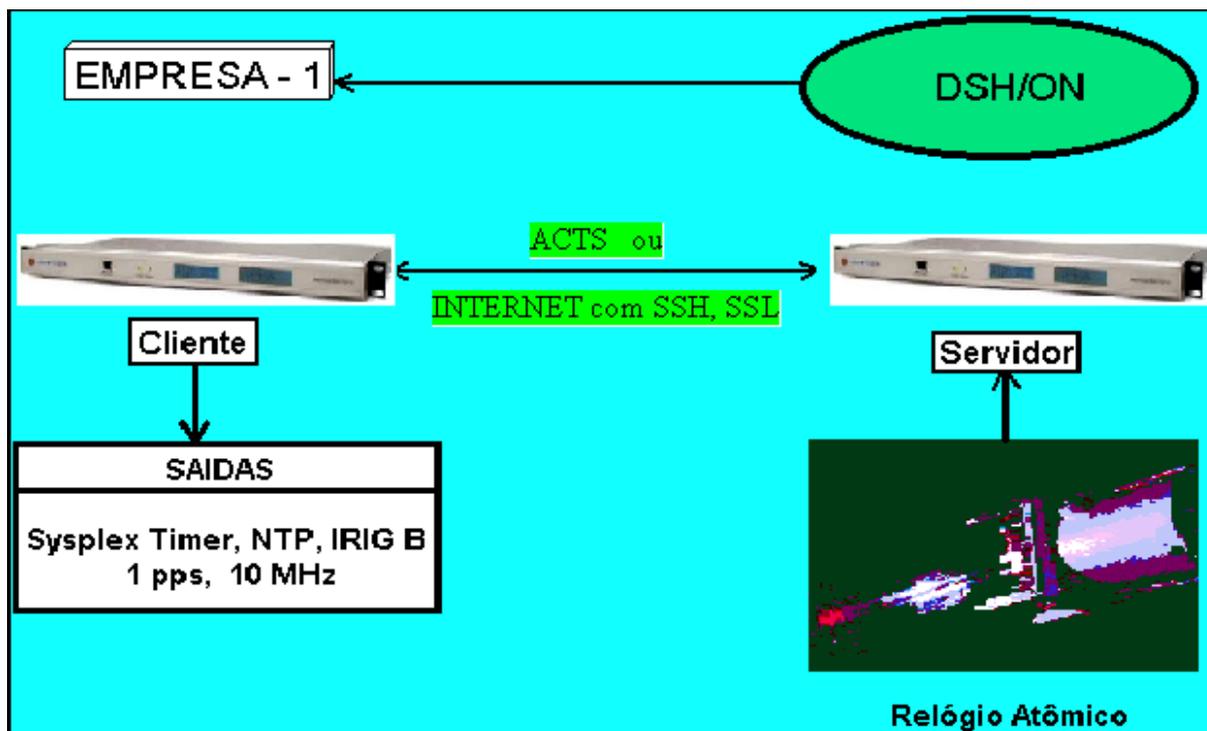


Figura 2 – Conexão ON <-> Cliente

3.2.1 - Sinais disponíveis no cliente

Alem da interface de rede 10/100 por intermédio de conector RJ45 CAT 5, o equipamento possui disponível as seguintes saídas:

RS-485 > Data/hora uma vez por segundo, ASCII 8N1

Contatos de Relés > Três relés, de alarme e de cronômetro programável

IRIG B > Modulado em amplitude, 1000 Hz; Codificado por largura de pulso, nível TTL

IRIG E > Modulado em amplitude, 1000 Hz; Codificado por largura de pulso, nível TTL

1 pps > Um pulso por segundo nível TTL, 50 ohms.

10 MHz > Sinal senoidal, 0,3 volts rms em 50 ohms

Na Figura 3 os tipos de sincronizações disponíveis nos clientes que estejam utilizando o ACTS. Temos saída para sincronismo de Mainframes por intermédio do Sysplex Timer, saída em interface RJ45 10/100 Mbits/s IPV4 ou IPV6, que possibilitam o sincronismo de servidores por intermédio do protocolo NTP com o recurso de autenticação por chaves simétricas no modo manual

ou por intermédio do sistema conhecido por “autokey”. O ON necessita de acessar o NetClock para obter os “logs” que por sua vez contem os registros dessas sincronizações.

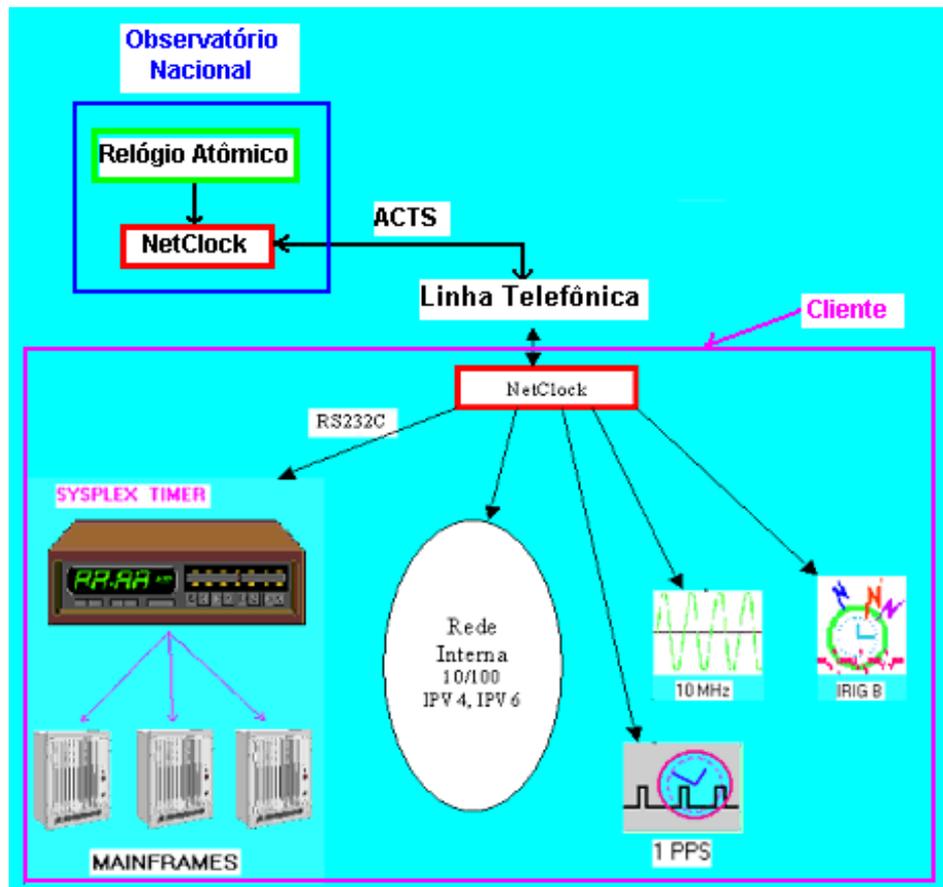


Figura 3 – Sincronizações nos clientes

Estes acessos do ON de realizam por intermédio do protocolo de segurança HTTPS. Os algoritmos de segurança utilizados no HTTPS são fornecidos pela livreria OpenSSL. Esta livreria também fornece ferramentas e programas utilizados para criar requisições de novos certificados, certificados auto assinados e duplas de chaves privadas/públicas. O equipamento vem com um certificado auto assinado de forma a poder ser utilizado imediatamente. O usuário pode criar um certificado auto assinado tipo x509, utilizando a interface WEB fornecida. Somente chaves do tipo RSA são suportadas. Também pode-se criar um “request” de certificado a ser enviado à uma Autoridade de Certificação – AC, para emissão de certificado e posterior instalação.

Podem ser criados e utilizados até 16 usuários diferentes.

Também podem ser utilizados como sistema de segurança os certificados digitais associados ao **Lightweight Directory Access Protocol – LDAP**, e a infra-estrutura **Remote Authentication Dial In User Service – RADIUS**, proporcionando os componentes de autenticação e autorização. Em ambos os casos estes recursos podem ser configurados pela interface WEB.

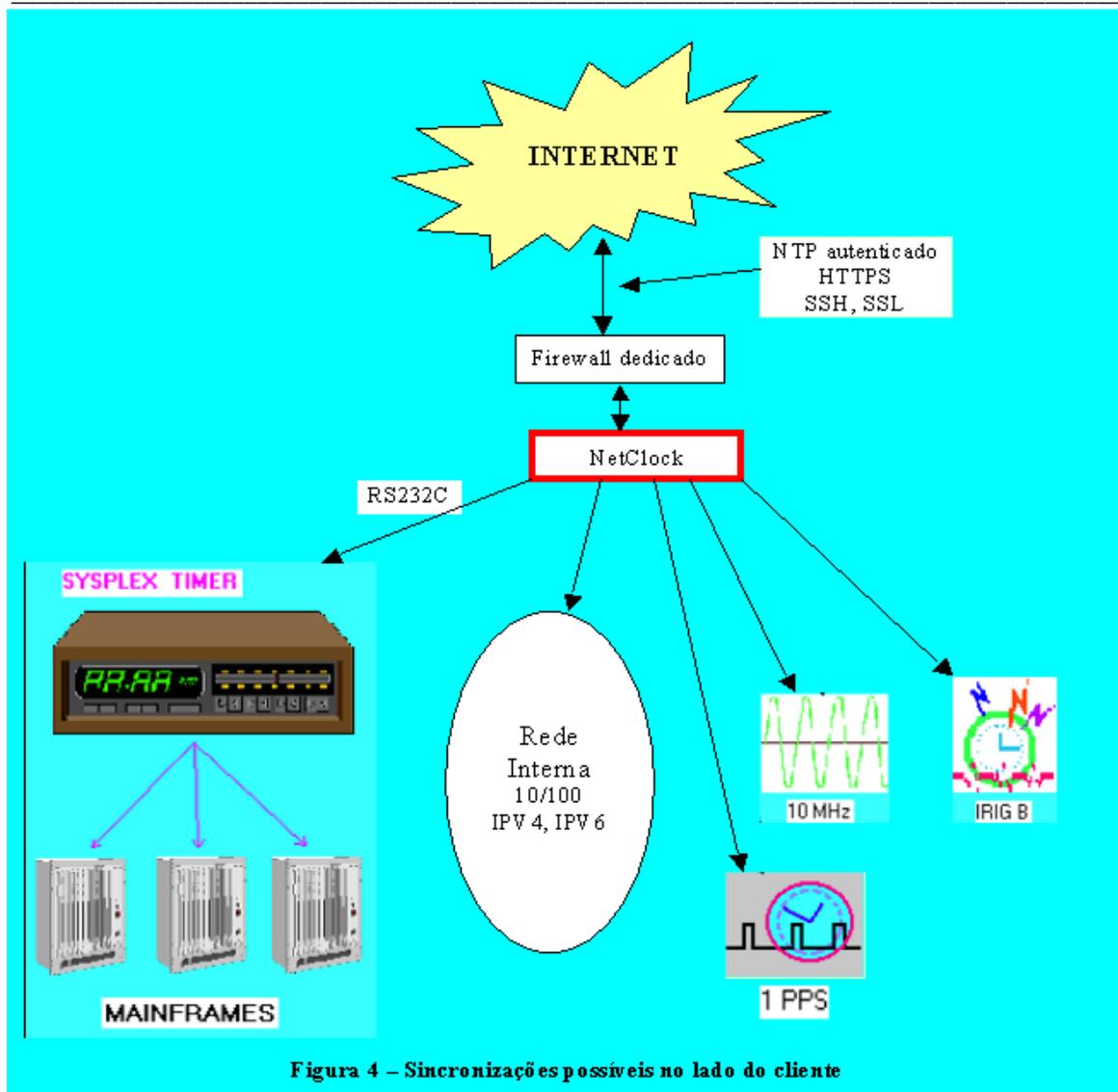


Figura 4 – Sincronizações possíveis no lado do cliente

3.3 - Especificações das Saídas do Equipamento (NetClock 9283)

3.3.1 - Interface de Rede

Ethernet 10/100BaseT auto sensing LAN, IEEE 802.3
Protocolos de tempo - NTP v4.2.0 com MD5 e Autokey, 4000 sincr/s ou 350 sincr/s (autenticado)
Outros protocolos - DHCP, HTTP, HTTPS, FTP, Syslog, SNMP, Telnet ;
HTTP/HTML com página de status; SNMP v1 com extensão MIB II;
SCP, SFTP, SSH, SSL, LDAP v2 e v3, RADIUS

3.3.2 - Conexões Seriais

Porta Setup - Tipo DCE RS-232C, com conector DB9 (fêmea), protocolo ACTS, 9600 baud, 8 bits, 1 start/stop, sem paridade (8N1), utilizada para configuração ou para se interligar ao modem.

Porta Serial 1 - Tipo DCE RS-232C, com conector DB9 (fêmea), para ligação ao SYSPLEX TIMER 9600 baud, 8 bits, 1 start/stop, paridade ímpar (8O1).

Porta RS-485 – Saída da data/hora uma vez por segundo, com conector removível, ASCII, velocidades disponíveis de 1200, 2400, 4800 e 9600 baud, 8 bits, 1 start/stop, paridade ímpar (8O1).

3.3.3 – Saídas de Reles

Três saídas separadas para alarmes ou eventos programados, 30 volts @ 2 A

3.3.4 – Saídas IRIG

Sinal:	IRIG B, ou IRIG E 50 Ω Modulado em amplitude (AM) ou Codificado por largura de pulso (DCLS) ou Codificado por largura de pulso (DCLS, diferencial)
Portadora AM:	IRIG B 1 kHz IRIG E 100 Hz ou 1 kHz
Nível AM:	Ajustável de 0 a 10 V_{pp} para cargas de 600 Ω ou mais. Valor de fábrica 2 V_{pp}
Nível DCLS:	TTL
Exatidão:	IRIG B, IRIG E 1kHz AM: $\pm 20 \mu s$ em relação à entrada de referência IRIG E 100 Hz AM: $\pm 200 \mu s$ em relação à entrada de referência IRIG B, IRIG E TTL: $\pm 2 \mu s$ em relação à entrada de referência IRIG B, IRIG E Diff: $\pm 2 \mu s$ em relação à entrada de referência
Conector:	AM, DCLS: fêmea BNC DCLS Diff: DB9 fêmea
Configuração:	IRIG B ou E em AM ou DCLS(TTL). Possível configurar os fusos e horário de verão.
Controle de Assinatura:	Esta configuração remove o sinal de saída sempre que a condição de alarme selecionada ocorrer.

3.3.5 – Saída de 1PPS

Sinal:	Onda quadrada de um pulso por segundo derivada da referência de entrada.
Nível de Sinal:	TTL, 1,5 V de 0 a pico em 50 Ω
Largura de pulso:	200 mili segundos
Exatidão:	Subida do pulso dentro de $\pm 100 ns$ em relação à entrada de referência
Conector:	BNC fêmea

3.3.6 – Saída de frequência

Sinal:	Onda senoidal de 10 MHz
Nível:	350 mVrms em 50 Ω .
Harmônicos:	no mínimo – 30DBc
Espúrios:	no mínimo – 35DBc
Exatidão:	TCXO (quartzo normal) 1×10^{-10} média de 24 horas. OCXO(quartzo câmara térmica) 1×10^{-11} média de 24 horas, envelhecimento de 2×10^{-9} por semana.
Conector:	BNC fêmea
Controle de Assinatura:	Esta configuração remove o sinal de saída sempre que a condição de alarme selecionada ocorrer ou quando houver perda de sincronismo.

3.3.7 – Saída RS-485

Sinal:	Data/hora uma vez por segundo em várias configurações.
Conector:	Bloco de terminais removível, 3 posições.
Formato:	ASCII 8N1
Exatidão:	$\pm 100 \mu s$ em relação à entrada de referência para os formatos 0, 1, 3 e 8, e $\pm 1 ms$ em relação à entrada de referência para os formatos 2, 4 e 7.
Configuração:	Formato (8 possibilidades) e velocidade de saída (1200, 2400, 4800 e 9600 baud) configurável por intermédio da interface WEB administrativa.

3.4 - Especificações das Entradas do Equipamento

3.4.1 – Entrada IRIG

Sinal:	IRIG B senoide modulada em amplitude (AM) ou pulso codificado por largura (DCLS, diferencial)
Portadora AM:	IRIG B 1 kHz
Nível AM:	500 mV _{pp} a 10 V _{pp} (Modulação de 2:1 até 6:1).
Nível DCLS:	TTL diferencial, >10k Ω.
Conector:	AM: BNC fêmea. DCLS Diff: DB9 fêmea.

3.4.2 – Entrada 1PPS

Sinal:	Onda quadrada de um pulso por segundo.
Nível:	TTL, referência na subida.
Conector:	BNC fêmea.

3.5 - Consumo de Energia

Fonte de energia:	90 a 240 VAC, 47 a 63 Hz.
Entrada DC:	9,5 a 30 VDC, 18 watts, por meio de adaptador fornecido com equipamento.
Conector:	Tipo Barrel, 5,5 mm diâmetro externo, 2,5 mm diâmetro interno.
Polaridade:	Centro positivo, externo negativo.

3.6 – Ambiente, Dimensões e Peso

Dimensões:	Rack de 19", Largura 483 mm, Altura 1U, profundidade 305 mm.
Peso:	2,7 kg.
Temperatura:	Operação de 0°C a 50°C.
Umidade:	de 10% a 95% de umidade relativa.

3.7 - Confiabilidade

MTBF = 56.000 horas

4 - EXATIDÃO DO TEMPO

Obviamente, a característica mais importante que um servidor de tempo deve possuir é a exatidão da hora fornecida, entendendo-se o termo exatidão como sendo a concordância da hora fornecida pelo servidor em relação à hora considerada correta a nível mundial. Esta hora por sua vez é o UTC, calculado e disponibilizado pelo BIPM, com sede na França.

O BIPM realiza este cálculo a partir de um conjunto de cerca de 200 padrões de Césio, pertencentes a diversos laboratórios de aproximadamente 50 países. Após os cálculos, as correções correspondentes a cada um dos padrões participantes são publicadas uma vez por mês, possibilitando que cada laboratório saiba qual a correção que deva ser aplicada em seu padrão para obter o UTC correto.

No Brasil a DSH do ON participa deste esquema desde que ele foi implantado inicialmente pelo BIH (Bureau International de l'Heure) e mais tarde pelo BIPM. Portanto a hora fornecida pelo DSH do ON, é rastreável ao BIPM e os documentos que demonstram esta rastreabilidade estão disponíveis na Internet no endereço <ftp://ftp2.bipm.org> (circular T). Nas circulares o DSH do ON é identificado como ONRJ.

CIRCULAR T 221
2006 JUNE 15, 11h UTC

ISSN 1143-1393

BUREAU INTERNATIONAL DES POIDS ET MESURES
ORGANISATION INTERGOUVERNEMENTALE DE LA CONVENTION DU METRE
PAVILLON DE BRETEUIL F-92312 SEVRES CEDEX TEL. +33 1 45 07 70 70 FAX. +33 1 45 34 20 21 tai@bipm.org

1 - Coordinated Universal Time UTC and its local realizations UTC(k). Computed values of [UTC-UTC(k)] and uncertainties valid for the period of this Circular. From 2006 January 1, Oh UTC, TAI-UTC = 33 s.

Date 2006	Oh UTC	APR 29	MAY 4	MAY 9	MAY 14	MAY 19	MAY 24	MAY 29
MJD		53854	53859	53864	53869	53874	53879	53884
Laboratory k					[UTC-UTC(k)]/ns			
NIST (Boulder)		6.4	7.0	6.4	6.2	6.5	6.6	6.5
NMC (Sofiya)		-4484.7	-4486.9	-4485.5	-4475.5	-4461.7	-4491.4	-4519.1
NMIJ (Tsukuba)		-9.9	-11.2	-13.2	-14.3	-15.3	-13.3	-12.5
NMLS (Sepang)		-347.2	-350.8	-353.0	-357.9	-366.1	-366.4	-358.0
NPL (Teddington)		40.1	36.3	32.7	28.0	26.8	23.2	20.0
NPLI (New-Delhi)		121.2	147.5	163.2	173.5	143.2	9.4	19.7
NRC (Ottawa)		19.4	17.0	17.9	1.2	3.5	10.6	1.2
NTSC (Lintong)		-0.4	-2.1	-3.4	-3.4	-2.8	-1.1	2.8
OMH (Budapest)		11046.3	11044.4	11059.5	11048.6	11071.5	11098.2	11099.1
ONBA (Buenos Aires)		-9703.0	-9736.1	-9718.5	-9725.9	-9794.6	-10007.7	-10137.8
ONRJ (Rio de Janeiro)		6889.2	6936.4	6997.2	7055.8	7108.3	7151.6	7203.9
OP (Paris)		-32.8	-35.0	-26.6	-25.9	-21.2	-14.4	-16.2

5 - SOLICITAÇÃO DE CONEXÃO

O solicitante deverá enviar correspondência para:

OBSERVATÓRIO NACIONAL
DIVISÃO SERVIÇO DA HORA
Rua Gal José Cristino, 77 São Cristóvão
Rio de Janeiro - RJ
CEP 20921- 400
Assunto : ReSinc/HLB
AC: Luiz Carlos do Carmo Motta

ou via e-mail para :

lccm@on.br e/ou dsh@on.br

5.1 - Informações necessárias

Nome ou Razão Social
Nome de Fantasia (se houver)
CNPJ
Inscrição estadual
Endereço Completo
Telefone, Fax
Nome e Cargo da pessoa para contato
e-mail

5.2 - Outras Providências

5.2.1 - Equipamentos a serem adquiridos

Se for utilizado o sistema com ACTS, refira-se à Tabela-1, se for utilizado o NTP autenticado, refira-se à Tabela-2.

Tabela –1 Conexão por ACTS

ITEM	DESCRIÇÃO	QTD
1	Linha de telefone fixo, normal.	1
2	Equipamento NetClock 9283 para sincronismo de tempo.	2
3	Modem externo compatível com comandos Hayes.	2
4	Cabo de conexão, tipo PC Modem DB9F/25M, com 1,8 metros	2

Tabela –2 Conexão por NTP autenticado

ITEM	DESCRIÇÃO	QTD
1	Firewall dedicado com interface WEB e gerenciamento remoto via VPN.	1
2	Equipamento NetClock 9283 para sincronismo de tempo.	2

5.2.2 – Equipamentos instalados

5.2.2.1 - Em local sob a responsabilidade do ON, sistema com ACTS

Um NetClock 9283, um modem e um dos cabos indicados no item 4 da Tabela-1.

5.2.2.2 - Em local sob a responsabilidade do ON, sistema com NTP autenticado

Um NetClock 9283, item 2 da Tabela-2.

5.2.2.3 - Nas dependências do solicitante, sistema com ACTS

Um NetClock 9283, um modem e um dos cabos indicados no item 4 da Tabela-1.

5.2.2.4 - Nas dependências do solicitante, sistema com NTP autenticado

Um Firewall, um NetClock 9283.