



Redes de Computadores 2014/2

Prof. Galvani Cavalcante

Aula HomePlug

arquivo imagens.zip

finalizar comentários filme Guerreiros da Internet

3 aulas para tirar dúvidas antes da P1

inscrição confirmada somente de 09 alunos

Assinaturas gratuitas

IP Journal

<http://www.internetsociety.org/ipj>

For more information or subscriptions

Send email to: ipj@protocoljournal.org

ORACLE MAGAZINE Free Subscription Form

<http://www.oracle.com/us/corporate/publishing/subscribe/index.html>

Atualizações de segurança

- <http://computerworld.com.br/seguranca/2014/11/07/microsoft-planeja-atualizacao-201cmonstro201d-de-seguranca/>

Microsoft planeja atualização 'monstro' de segurança

A última vez que a fabricante havia lançado um pacote com tantas atualizações foi em abril de 2011, quando liberou 17 updates

07 de novembro de 2014 - 10h11

Atualizar firewalls, aumento varreduras de portas (nmap), ambiente de homologação antes de liberar para Servidores de Produção e estações de trabalho

Atualizações de segurança

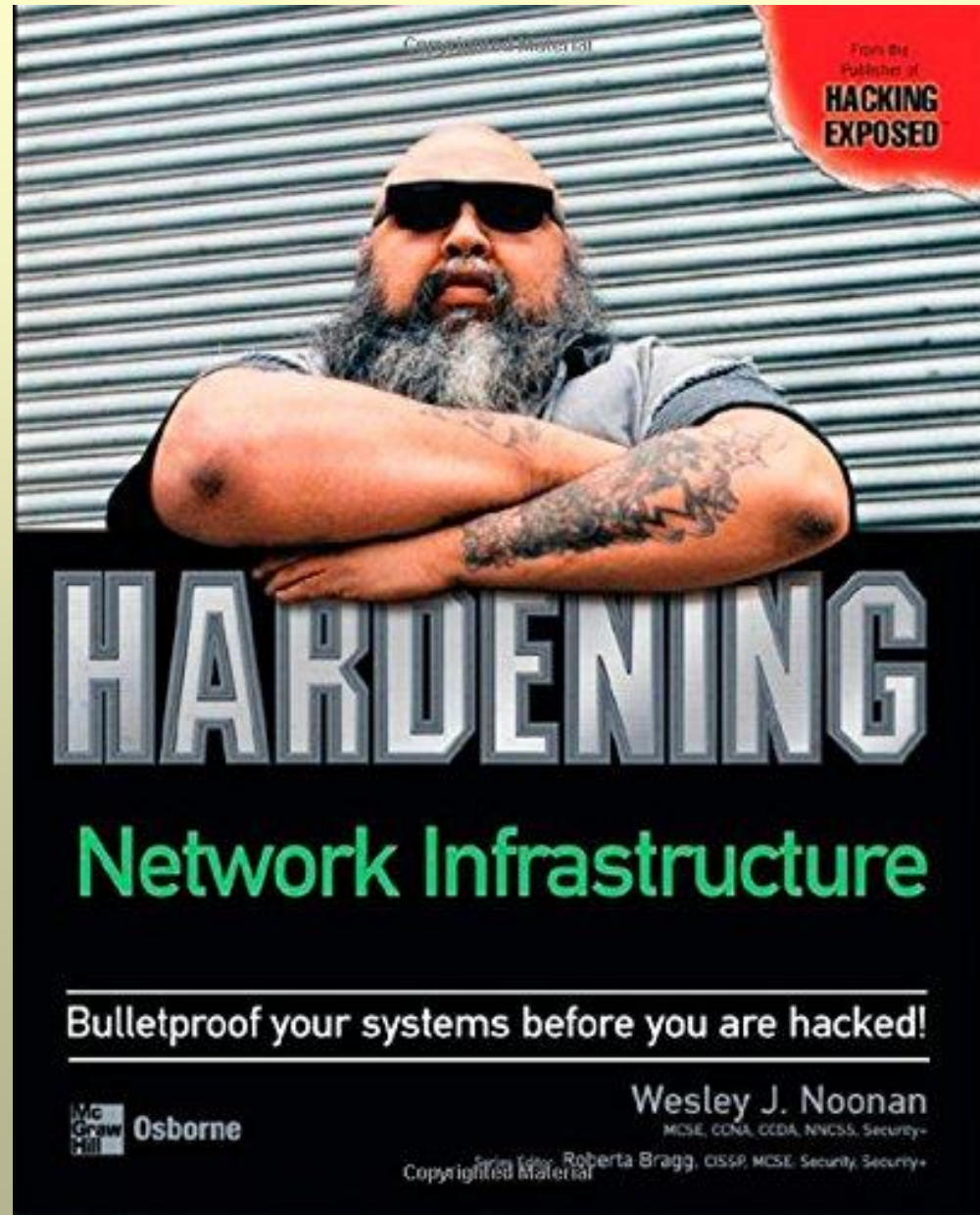
- https://www.kb.cert.org/CERT_WEB/services/vul-notes-cert.nsf/b38c0892d481f5d385256d4b005d34ea/dfdc369c328908e985257179006cb343?OpenDocument
- Vulnerability Note VU#317350, ISC DHCP contains a stack buffer overflow vulnerability in handling log lines containing ASCII charac only, 22-Jun-2004
- <http://seclists.org/isn/2004/Jun/110>
- [SA11933] Fedora update for dhcp , Released: 2004-06-24
- Critical: Moderately critical Where: From local network
- Impact: System access, DoS
- <https://technet.microsoft.com/en-us/library/security/ms04-042.aspx>
- **Microsoft Security Bulletin MS04-042 – Important, Vulnerability in DHCP Could Allow Remote Code Execution and Denial of Service (885249)**
- Published: December 14, 2004

Hardening

- <http://re.granbery.edu.br/artigos/Mzk3.pdf>
- **Hardening em Sistemas Operacionais GNU/LINUX**
- <http://pt.wikipedia.org/wiki/Hardening>
- ***Hardening*** é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na [infraestrutura](#) e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- Normalmente, o processo inclui remover ou desabilitar nomes ou [logins](#) de usuários que não estejam mais em uso, além de serviços desnecessários.
- Outras providências que um processo de hardening pode incluir: limitar o [software](#) instalado àquele que se destina à função desejada do sistema; aplicar e manter os [patches](#) atualizados, tanto de [sistema operacional](#) quanto de aplicações; revisar e modificar as permissões dos sistemas de [arquivos](#), em especial no que diz respeito a escrita e execução; reforçar a segurança do login, impondo uma política de [senhas](#) fortes

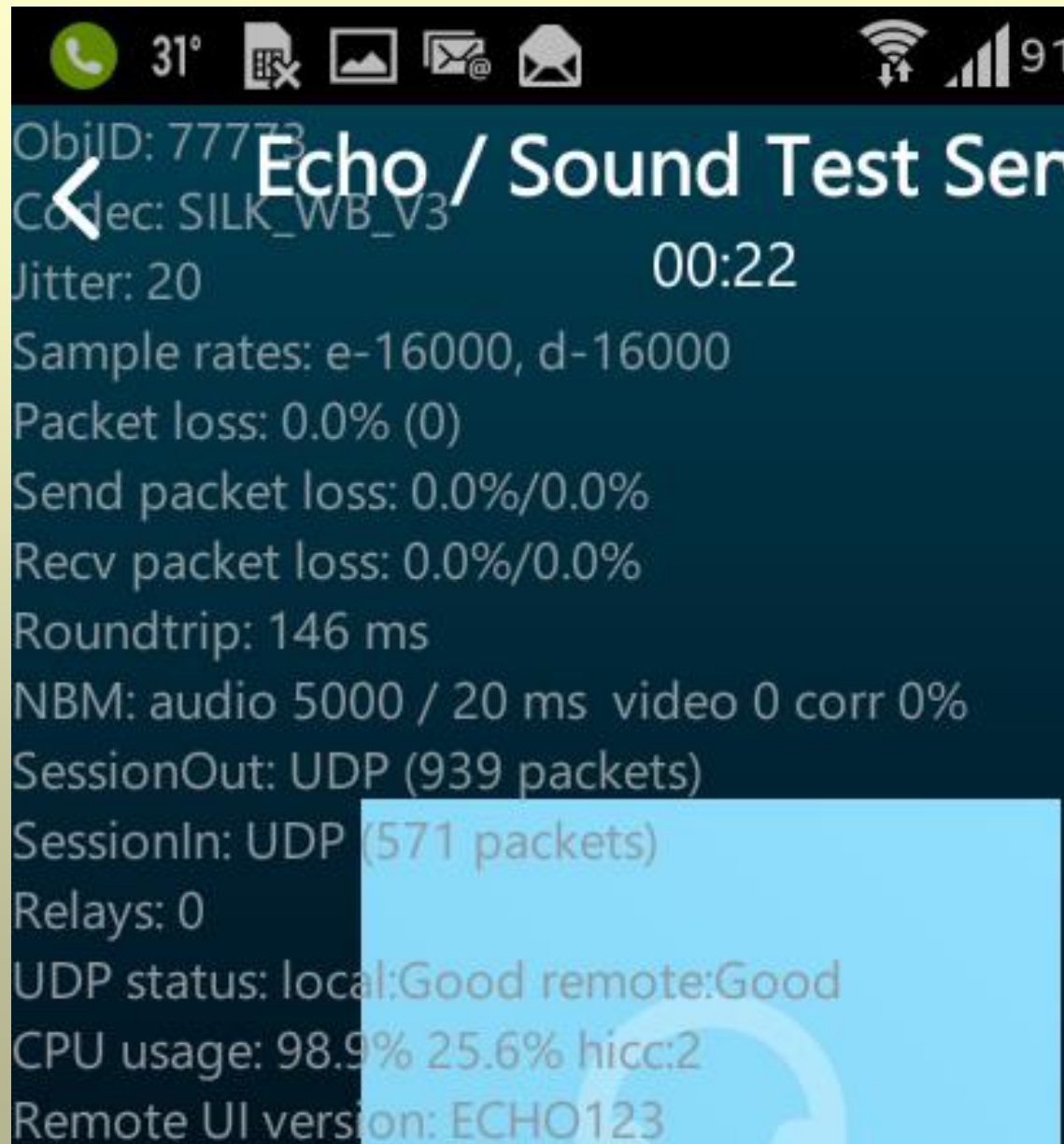
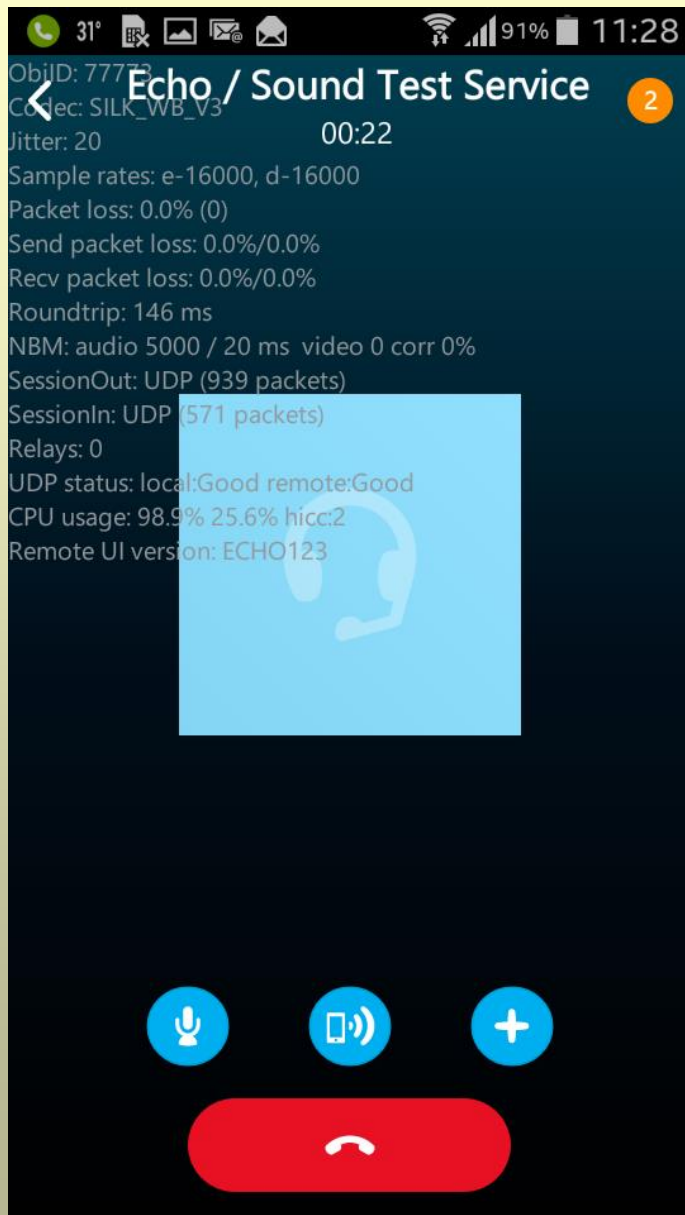
Hardening

- <http://www.amazon.com/Hardening-Linux-James-Turnbull/dp/1590594444>
- <http://www.amazon.com/Hardening-Windows-Systems-Roberta-Bragg/dp/0072253541>
- http://www.amazon.com/Hardening-Network-Infrastructure-Wes-Noonan/dp/0072255021/ref=sr_1_1?s=books&ie=UTF8&qid=1415556702&sr=1-1&keywords=hardening+network+infrastructure

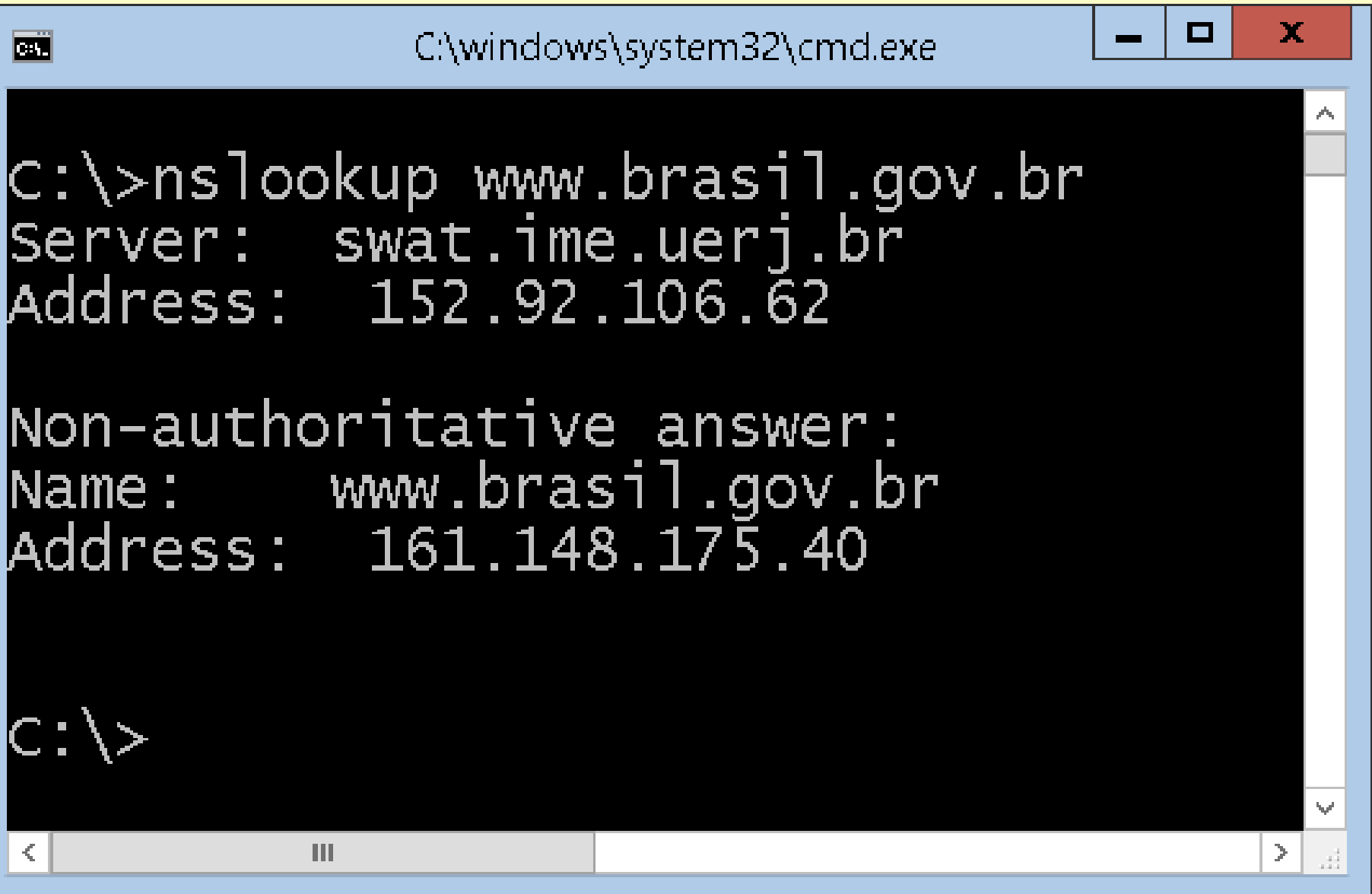


Dúvidas de sala de aula: UDP (VoIP)

atraso de 14 centésimos
(envio do pacote e
processamento dele pelo SO)



Dúvidas de sala de aula: UDP (DNS)



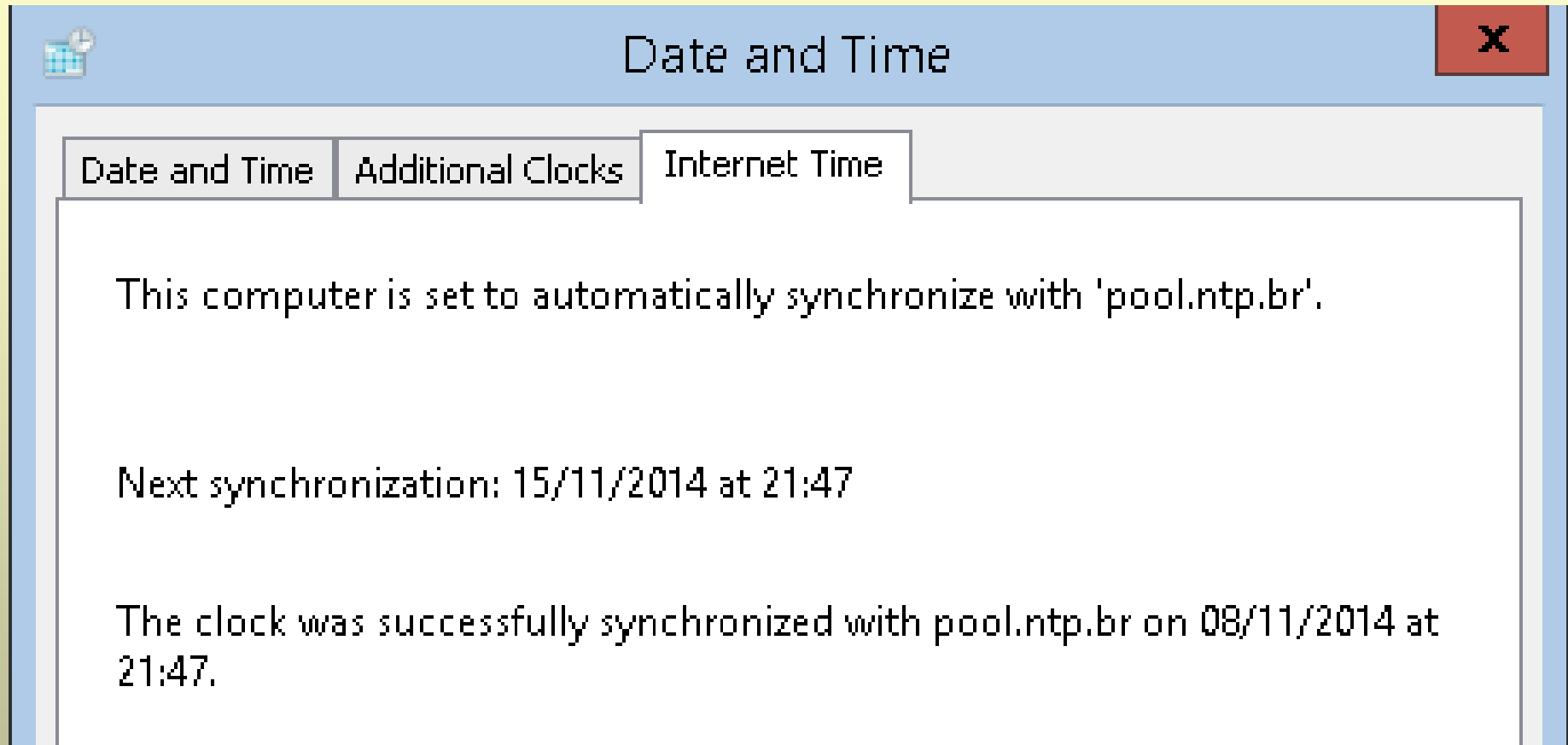
A screenshot of a Windows command prompt window. The title bar shows the path "C:\windows\system32\cmd.exe" and standard window controls. The command prompt displays the output of the "nslookup" command for the domain "www.brasil.gov.br". The output shows the server used ("swat.ime.uerj.br") and the IP address ("152.92.106.62"). It also shows a "Non-authoritative answer" with the same domain and a different IP address ("161.148.175.40"). The prompt is currently at "C: \>".

```
C:\>nslookup www.brasil.gov.br
Server:      swat.ime.uerj.br
Address:     152.92.106.62

Non-authoritative answer:
Name:        www.brasil.gov.br
Address:     161.148.175.40

C: \>
```

Dúvidas de sala de aula: UDP (NTP)



Dúvidas de sala de aula: rastreamento da navegação do usuário

<http://www.correio24horas.com.br/detalhe/noticia/acidente-com-onibus-na-br-101-deixa-sete-mortos-com-uma-crianca-e-28-feridos>

<http://www.correio24horas.com.br/detalhe/noticia/acidente-com-onibus-na-br-101-deixa-sete-mortos-com-uma-crianca-e-28-feridos/?cHash=00e5c302e0acc94909c79b8f1ce9dbfa>

Dúvidas de sala de aula: segurança em Câmeras IP

Site transmite imagens de 73 mil câmeras de segurança que usam senha padrão - No Brasil são 1,2 mil equipamentos que deveriam proteger, mas expõem a privacidade de seus donos 07/11/2014

<http://oglobo.globo.com/sociedade/tecnologia/site-transmite-imagens-de-73-mil-cameras-de-seguranca-que-usam-senha-padrao-14499975>

<http://info.abril.com.br/noticias/seguranca/2014/11/site-sinistro-transmite-ao-vivo-imagens-de-mais-de-70-mil-cameras-pelo-mundo.shtml>

<http://www.insecam.com/cam/bycountry/BR/?page=2>

<http://www.insecam.com/>

Sometimes administrator (possible you too) forgets to change default password like '*admin:admin*' or '*admin:12345*' on security surveillance system, online camera or DVR. Such online cameras are available for all internet users. Here you can see thousands of such cameras located in a cafes, shops, malls, industrial objects and bedrooms of all countries of the world. To browse cameras just select the country or camera type.

Dúvidas de sala de aula: segurança em camadas nas Câmeras IP

Nível 7: usuário e senha, vulnerabilidades protocolo HTTP, uso de certificados SSL para permitir criptografia no envio dos dados

Nível 4: liberar/bloquear acesso as portas TCP e UDP utilizadas pela câmera

Nível 3: restrição de faixa de endereços IPs que podem acessar a câmera

Nível 2: uso de QOS para diminuir atrasos no envio dos pacotes de áudio/vídeo

Nível 1: definição da tecnologia de transmissão de dados (ethernet, wifi); uso de PoE; Wifi possui vazão variável e muitas perdas; local de instalação: residência (Wifi), agência bancária (cabeadas); (re)configuração local do equipamento caso alguém tenha acesso físico ao dispositivo; banda mínima de 256Kpbs

Redes sem fio - questões

- 1) Que tipo de rede sem fio não usa WAP (Wireless Access Point)?
 - A) infra estruturada
 - B) Bus
 - C) Star
 - D) Ad hoc
- Lembrar de jogos multiusuário em rede, compartilhamento de internet pelo celular com acesso 3G e Wifi

Redes sem fio - questões

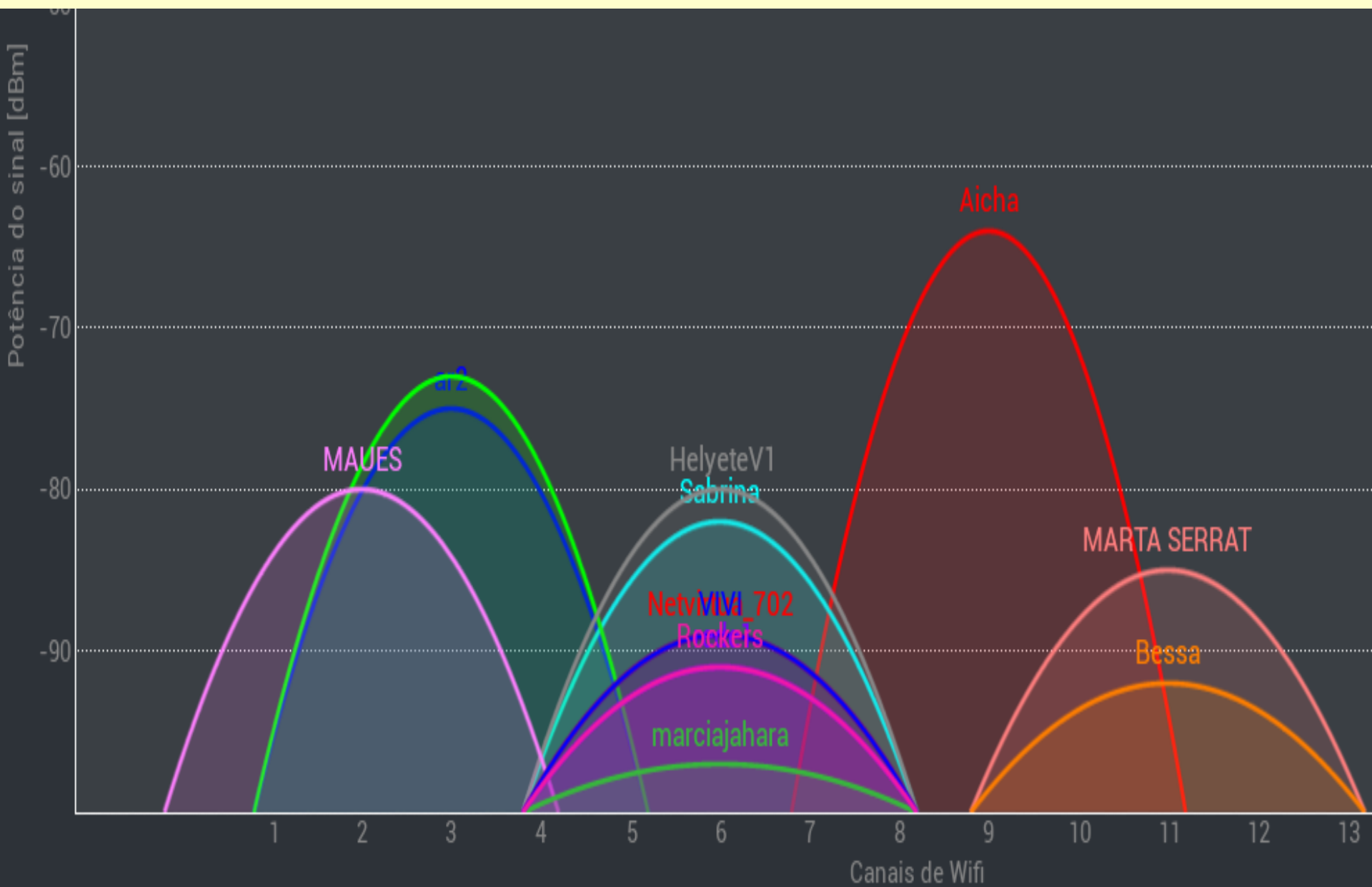
2) Que tecnologias permitem que o padrão IEEE 802.11n aumente dramaticamente a largura de banda? Escolha 02.

- A) Lempel-Ziv (LZ) compression
- B) Time-division multiplexing (TDMA)
- C) MIMO (múltiplas antenas no envio e na recepção)
- D) Channel bonding (uso de 2 canais de forma simultânea)

Redes sem fio - questões

3) Você ira implementar uma rede sem fio numa firma de contabilidade. O que você deverá configurar para aumentar a segurança desta rede?

- A) Implementar codificação (criptografia) WEP em todos os WAPs e em todos os clientes da rede sem fio.
- B) Esconder o SSID.
- C) Implementar codificação WPA em todos os WAP (Wireless Access Points) e em todos os clientes.
- D) implementar o software de criptografia Bit Locker



Redes sem fio - questões

4) Você descobriu que o sinal da sua rede sem fio está sendo emanado para o estacionamento de carros do outro lado da rua. Como evitar que o sinal seja propagado até lá? Escolha três.

- A) implementar “wireless repeaters” espalhados em áreas estratégicas de sua empresa
- B) reposicionar o WAP num ponto central do escritório.
- C) Incrementar o ganho da antena do WAP.
- D) Reduzir o parâmetro “power level” no WAP
- E) Implementar uma gaiola de Faraday (Faraday cage) no exterior do prédio.



TP-LINK®

Model: TL-WA860RE

**300Mbps WiFi Range Extender
with AC Passthrough**

Default Access: <http://tplinkextender.net>

Username: admin Password: admin

Input: 100-240V~ 50/60Hz 15.1A
(0.1A, product only)

Output: 15A Maximum load

FCC ID: TE7WA860RE IC: 8853A-WA860RE



CE 1588



MAC Address: E8DE272E0372



Model: TL-WA860RE(EU) Ver: 1.0

S/N: 2146306004843

MADE IN CHINA

EAC



Gaiola de Faraday

Gabinetes de computador, salas cofre, sala de comunicação de subestações de energia elétrica (locais envoltos por superfícies metálicas em todos os lados)

<http://physics2life.blogspot.com.br/2008/11/faraday-cage.html>

<http://www.survivalistboards.com/showthread.php?t=266663>

Blindagem eletroestática

<http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=25102>

http://www.intract.com.br/catalogo/loja_tipo2.php?cat_id=33

http://www.intract.com.br/catalogo/loja_tipo2.php?cat_id=33&pro_id=294



http://www.intract.com.br/catalogo/loja_tipo2.php?cat_id=33&pro_id=294

http://www.int...33&pro_id=294

www.intract.com.br/catalogo/loja_tipo2.php?cat_id=33&pro_id=294


Google

Nenhum item no carrinho

Ver carrinho :::>>

ESD - MATERIAIS ANTIESTÁTICOS >> Armazenamento >>

Detalhe: EMBALAGEM METALIZADA 25,4 x 30 cm(GAIOLA DE FARADAY)



EMBALAGEM METALIZADA 25,4 x 30 cm(GAIOLA DE FARADAY)

Saco Metalizado, METAL-IN 10X12 polegadas (25,4 x 30 cm)

Sob Consulta

- > Com camada interna de alumínio.
- > Dissipativo.
- > Visibilidade interna maior 40%.
- > Fabricado em processo totalmente automatizado.
- > Com selo de garantia do fabricante



Autor: Guilherme Dal Moro

Redes sem fio - questões

5) Sua rede sem fio esta com bastante interferência, com perda de conexões. Você descobriu que um telefone sem fio esta operando na faixa de 2,4GHz no canal 3 (inglês: cordless phone system, espanhol: inalámbrico). A empresa do andar de cima usa Wifi nos canais 1 e 5. O que você deverá fazer?

- A) Configurar o WAP para o canal 2.
- B) Configurar o WAP para o canal 7.
- C) Configurar o WAP para o canal 10.
- D) Configurar o WAP para o canal 15.

- **Já aconteceu com vocês do portão automático abrir sozinho?**

<https://br.answers.yahoo.com/question/index?qid=20081006123104AAn4yFa>

- **06/04/2014 22h13 - Aparelho que bloqueia travamento de carros é nova arma dos bandidos**

Dispositivo conhecido como 'Chapolin' é vendido no meio da rua no RS. Veja como evitar que você seja mais uma vítima desse tipo de golpe.

<http://g1.globo.com/fantastico/noticia/2014/04/aparelho-que-bloqueia-travamento-de-carros-e-nova-arma-dos-bandidos.html>

Primary Wireless Settings

Primary Wireless Network:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Broadcast Primary SSID:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
SSID:	<input type="text" value="rede-sem-fio"/>	
Password:	<input type="text" value="senha"/>	
Security Mode:	<input type="text" value="WPA2-PSK (AES)"/>	
WPS:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Registration Mode:	<input checked="" type="radio"/> Push Button	<input type="radio"/> Pin Number

General Wireless Settings

Interface Type:	<input type="text" value="Auto B/G/N"/>	
Channel:	<input type="text" value="13"/>	
Channel Bandwidth:	<input type="text" value="20"/>	
Transmit Power (%):	<input type="text" value="100"/>	
WMM:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
WMM Power Save:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Physical Address (MAC):	6c:2e:85:ea:6d:3d	
Frequency Band:	2.4Ghz	

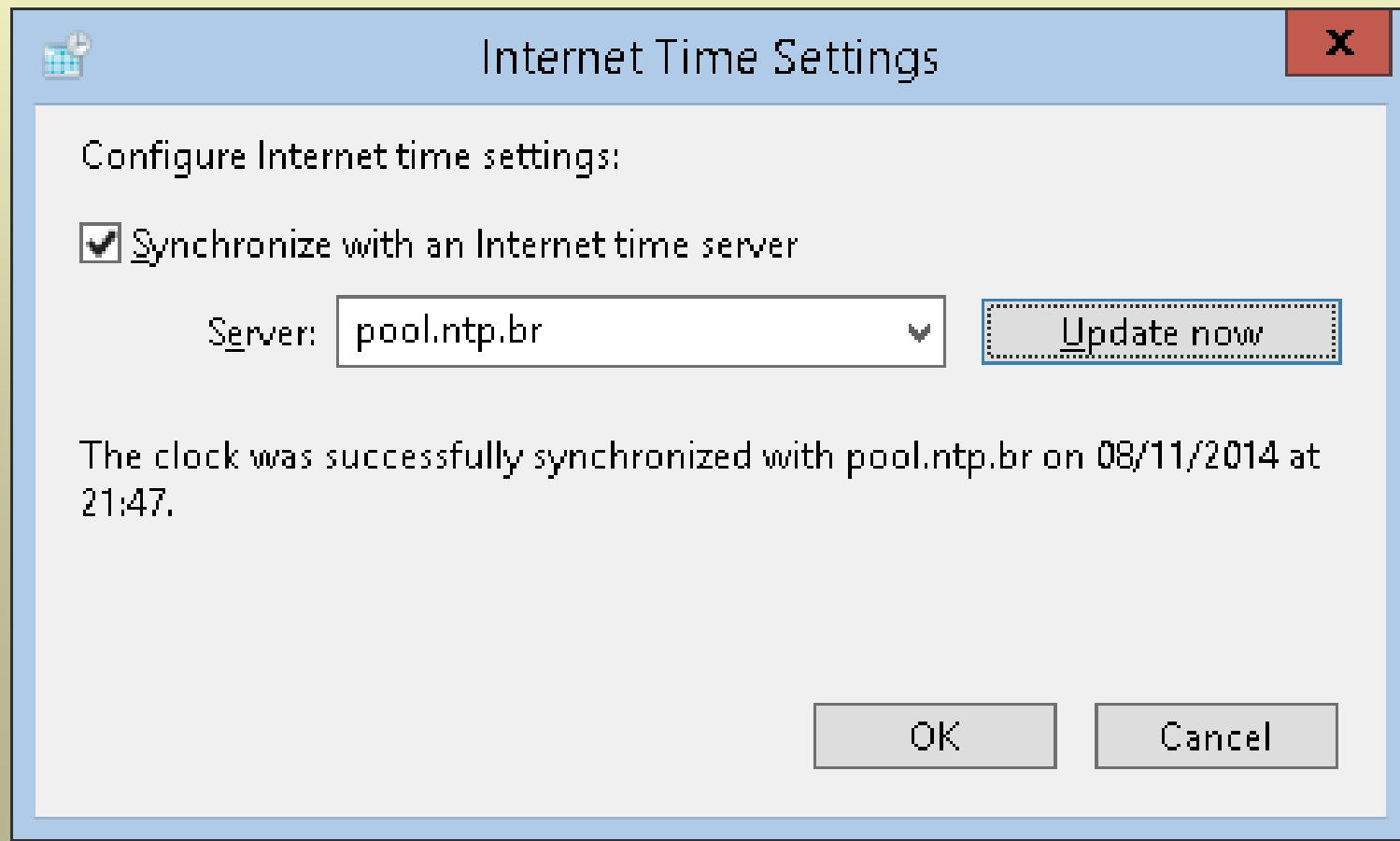
<http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/10/como-trocar-o-canal-da-sua-rede-wi-fi-evitando-interferencias.html>

Protocolo de Hora de Rede (NTP)

Protocolo NTP - Ajustar a Hora do Sistema - Linux LPIC-1

<http://www.youtube.com/user/bosontreinamentos/>

http://youtu.be/CuupIBX-F_s





Protocolo NTP

O Network Time Protocol

É um tipo de protocolo utilizado para sincronizar relógios de computadores, por meio de um grupo de computadores que dialogam entre si para acertar os relógios via UDP.

<http://mundolinux.pro.br/wp-content/uploads/2013/07/Protocolo-NTP.ppt>



Protocolo NTP

O **NTP** propicia a hora certa nos relógios dos computadores com exatidão.

Na Internet vários computadores de diferentes regiões troca de informação entre si, o que exige uma exatidão de hora, sem que a hora de um computador ou terminal de dados interfira na informação real do local em que está instalada a máquina.



Protocolo NTP

Em determinados softwares ocorrem erros que geram atrasos e adiantamentos dos relógios por um determinado período, à revelia do próprio usuário.

Dentre os aplicativos que podem ser afetados são o Sistema de distribuição de conteúdo; Sistemas de arquivos; Agendadores de eventos; Criptografia; Protocolos de comunicação; Sistemas transacionais e banco de dados.



Protocolo NTP

Para proteger a segurança de uma rede é necessário a constante sincronização dos relógios:

Investigar incidentes no sistema de seguranças.

A ordem de segundos e milésimas diferenças de segundos entre os relógios são atitudes usadas em algumas aplicações.

Consultar o tempo do servidor e realizar ajustes no relógio local, o NTP é responsável por buscar informações de tempo do servidor relacionadas ao deslocamento, dispersão e variação.

O NTP também analisa qual servidor fornece o tempo mais preciso.

Utiliza métodos criptográficos para prevenir ataques contra os servidores, e sincroniza informação de tempo com outros servidores NTP.



Protocolo NTP

A Rede Nacional de Ensino e Pesquisa (RNP) em seu centro de atendimento a incidentes de segurança, no ano de 2000, implantou um serviço de NTP, ligado diretamente ao um relógio de referência, que utiliza um receptor de GPS – Global Positioning System – estruturado numa hierarquia de servidores NTP para a distribuição da carga de processamento.



Protocolo NTP

Os servidores do NTP.br são os seguintes:

Nome	Endereço
a.st1.ntp.br	200.160.7.186 e 2001:12ff:0:7::186
b.st1.ntp.br	201.49.148.135
c.st1.ntp.br	200.186.125.195
d.st1.ntp.br	200.192.232.8
a.ntp.br	200.160.0.8 e 2001:12ff::8
b.ntp.br	200.189.40.8
c.ntp.br	200.192.232.8
gps.ntp.br	200.160.7.193 e 2001:12ff:0:7::193



Protocolo NTP

Links uteis de configuração

<http://www.ntp.br/NTP/MenuNTPLinks>

<http://www.ntp.br/NTP/MenuNTPWindows>

<http://www.ntp.br/NTP/MenuNTPLinuxBSD>

<http://www.ntp.br/NTP/MenuNTPMac>



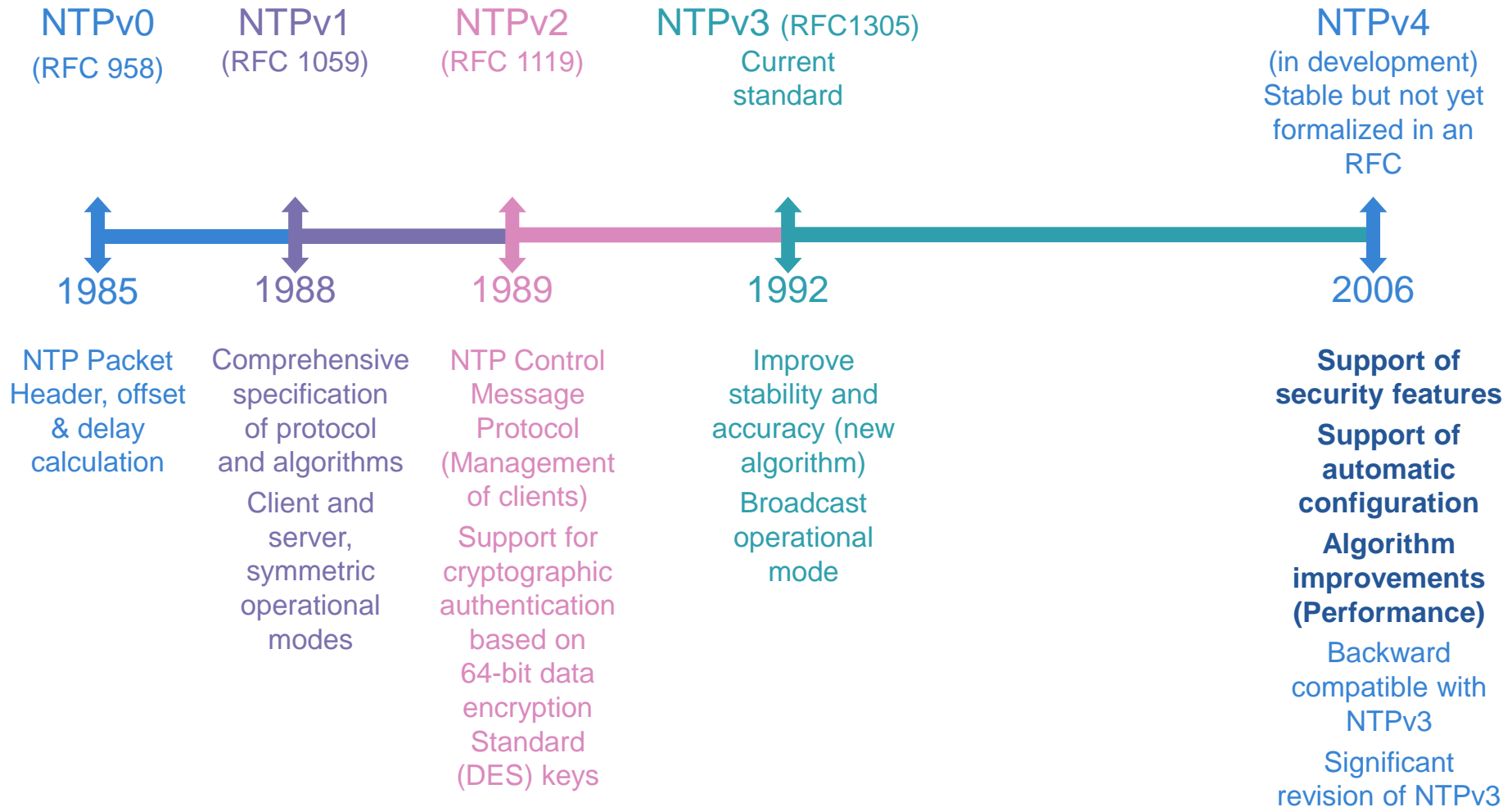
Enhanced NTP

IETF – TicToc BOF

Greg Dowd – gdowd@symmetricom.com

Jeremy Bennington – jbennington@symmetricom.com

A Brief History of NTP



Hora Legal Brasileira

<http://ntp.br/>

Horário de Verão (de GMT -3 para GMT -2)

<http://pcdsh01.on.br/verao1.html>

Hora falada

<http://pcdsh01.on.br/TelefoneDedicadoDifusaoHora.html>

+55-21-2580-6037

Manter os dispositivos nas redes e na Internet com a hora certa é muito importante. Isso vale para servidores, roteadores, notebooks e desktops! Muitas aplicações dependem disso para funcionar bem. Incidentes de segurança e até crimes cibernéticos só podem ser investigados se os *logs* dos dispositivos envolvidos estiverem em sincronismo.

Por um acordo entre o **ON (Observatório Nacional)**, que é responsável pela Hora Legal Brasileira, e o **NIC.br (Núcleo de Informação e Coordenação do Ponto BR)**, a hora certa no Brasil é distribuída gratuitamente via Internet por meio do NTP.br. Saiba mais navegando pelo [sítio](http://ntp.br), e utilize livremente os servidores disponíveis:

a.st1.ntp.br	b.st1.ntp.br	c.st1.ntp.br	d.st1.ntp.br
a.ntp.br	b.ntp.br	c.ntp.br	gps.ntp.br

Se você usa uma versão recente (4.2.6 ou superior) do *NTPd*, ou o *OpenNTPD*, pode usar também o seguinte *pool* DNS, para configurar todos os servidores de uma só vez:

pool.ntp.br

Configure os servidores na configuração global. O ideal é que você use seus servidores ntp locais, que já estarão sincronizados com o ntp.br. Mas se sua rede for pequena e você não tiver servidores ntp locais, pode utilizar os servidores do NTP.br diretamente:

```
ntp server a.st1.ntp.br
ntp server b.st1.ntp.br
ntp server c.st1.ntp.br
ntp server d.st1.ntp.br
ntp server gps.ntp.br
ntp server a.ntp.br
ntp server b.ntp.br
ntp server c.ntp.br
```

```
ntp server 110.17.72.34 version 2
ntp server 110.21.72.31 version 2 prefer
```

Desabilite o serviço ntp nas interfaces onde não for necessário (interfaces externas, por exemplo):

```
interface Eth0
ntp disable
```

Indique a interface que será utilizada para o ntp

```
ntp source Eth0
```

É possível verificar o funcionamento do ntp utilizando os comandos:

```
show ntp status
show ntp associations
```

Network Time Protocol - NTP

Lizandro Damian Solano-Quinde

<http://www.ee.iastate.edu/~gmani/cpre545/lectures/students-07/ntp.ppt>

NTP - Introduction

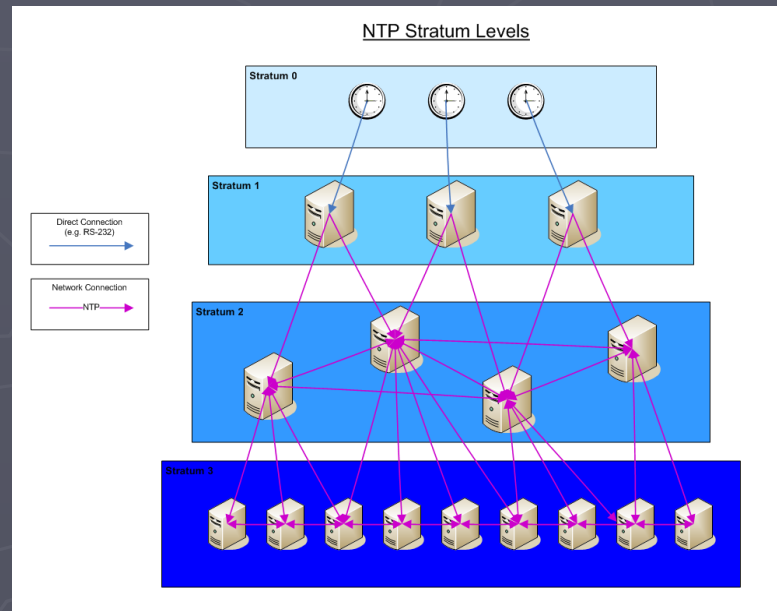
- ✓ NTP is a protocol for synchronizing the clocks on computers over packet-switched data networks
- ✓ NTP delivers accurate and reliable time in spite of faults in the network
- ✓ Provides a connectionless service (UDP in the Transport Layer)
- ✓ NTP is used on Internet

NTP - Clock Stratum

- ✓ NTP uses a hierarchical organization of clocks
 - Stratum 0.- Composed by: Atomic Clocks, GPS Clocks.
 - Stratum 1 - Primary
 - Time Servers.- Computers attached to stratus 0 devices
 - They act as servers for requests from Stratus 2
 - Stratum 2
 - Computers sending NTP requests to Time Servers in Stratum 1
 - Computers in this level will reference to several time servers to synchronize their clocks
 - S2 Computers will peer with another S2 computers to provide more reliable and robust time for all devices in the peer group
 - They act as servers for requests from Stratus 3

NTP - Clock Stratum

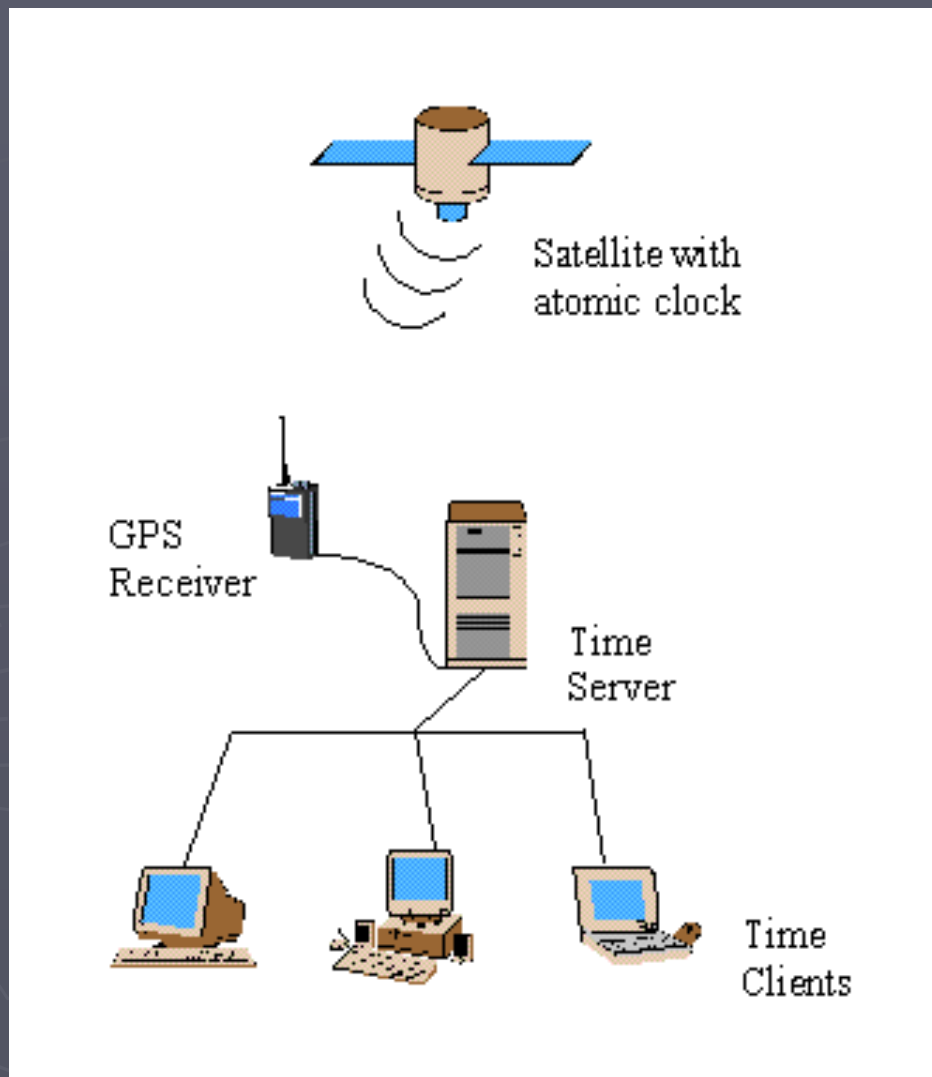
- Stratum 3, 4, ...
 - Computers employ the same NTP function as in Stratum 2
 - Potentially up to 16 levels



* Image taken from www.wikipedia.com

Satélites GPS

<http://www.bytefusion.com/products/ntm/ptnt/gpstimesynchronization.htm>

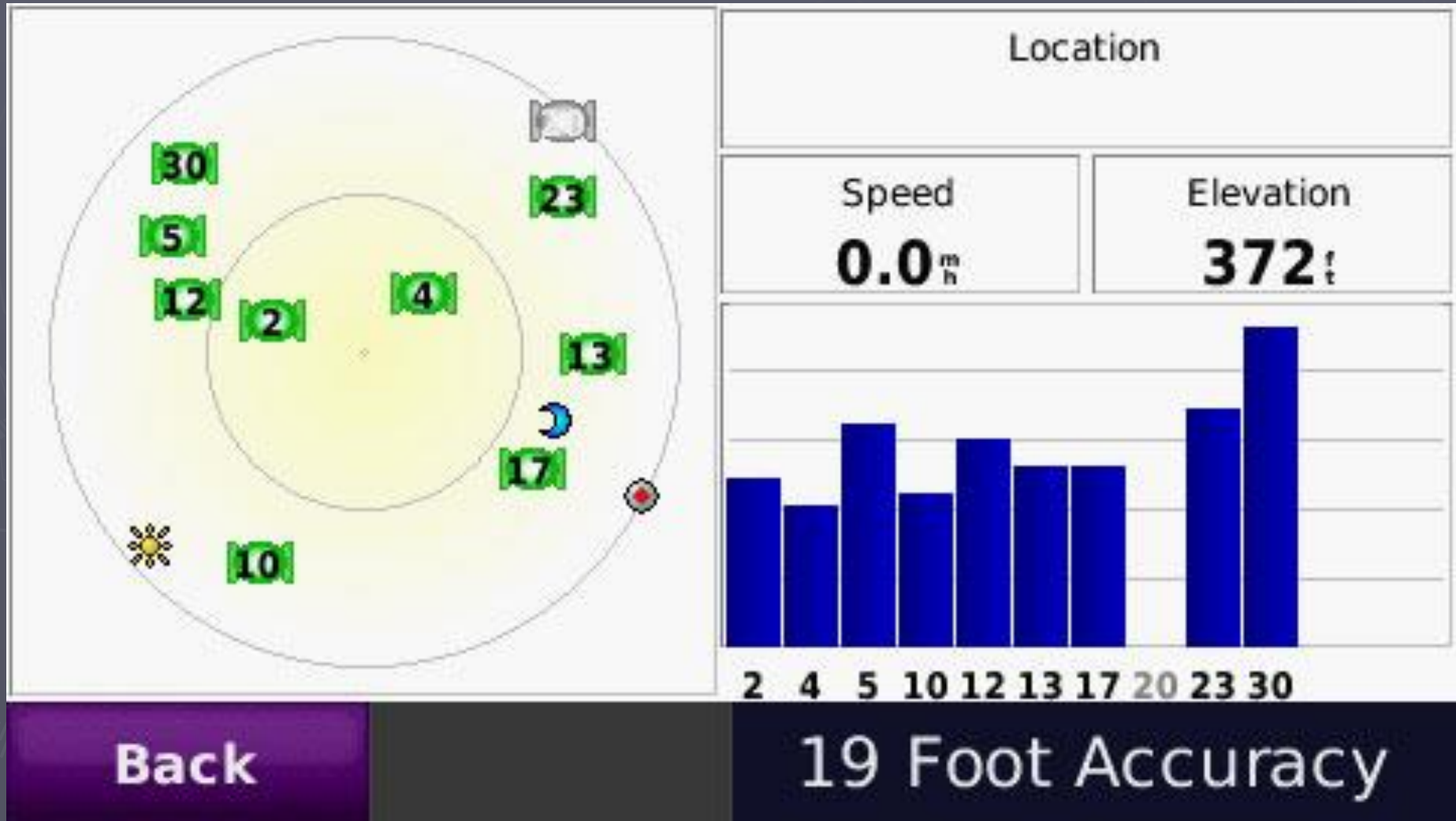




<http://www.gpsreview.net/satellite-info-screen/>

30,48cm x 19 = 5,80m de precisão

(x,y) = (latitude, longitude)



Rede Mundial para embarcações no mar

<http://www.mar.mil.br/dhn/chm/box-publicacoes/publicacoes/lar/04-LAR-Cap03-Sinais-horarios.pdf>

Rádio-Difusão de Sinais Horários

<http://pcdsh01.on.br/RadioDifusaoSinaisHorarios.html>

A DSHO dissemina a Hora Legal Brasileira via rádio-difusão no fuso horário de Brasília nas frequências de 10 MHz, 166,53 MHz e 171,13 MHz.

clock "radio controlled"

<http://www.nist.gov/pml/div688/grp40/radioclocks.cfm>

<http://tfa-dostmann.de/index.php?id=138&L=1>

http://tfa-dostmann.de/fileadmin/-----Anleitungen-----/98.1038_multi.pdf

Relógio de cabeceira

[http://tfa-dostmann.de/index.php?eID=tx_cms_showpic&file=uploads%2Ftx_prodkat%2F981038gross_01.jpg&md5=9d920c173735c43981654469c5b8f7affa91e92¶meters\[0\]=YTo0OntzOjU6ln dpZHRoljtzOjQ6IjEwMjQiO3M6NjoiaGVpZ2h0IjtzOjQ6IjEw¶meters\[1\]=MjQiO3M6NzoiYm9keVRhZyl7czoyNDoiPGJvZHkgYmdDb2xvcj0il2ZmZmZmZil%2B¶meters\[2\]=IjtzOjQ6Indy YXAiO3M6Mzc6IjxhIGhyZWY9Imphd mFzY3JpcHQ6Y2xvc2UoKTsi¶meters\[3\]=PiB8IDwvYT4iO30%3D](http://tfa-dostmann.de/index.php?eID=tx_cms_showpic&file=uploads%2Ftx_prodkat%2F981038gross_01.jpg&md5=9d920c173735c43981654469c5b8f7affa91e92¶meters[0]=YTo0OntzOjU6ln dpZHRoljtzOjQ6IjEwMjQiO3M6NjoiaGVpZ2h0IjtzOjQ6IjEw¶meters[1]=MjQiO3M6NzoiYm9keVRhZyl7czoyNDoiPGJvZHkgYmdDb2xvcj0il2ZmZmZmZil%2B¶meters[2]=IjtzOjQ6Indy YXAiO3M6Mzc6IjxhIGhyZWY9Imphd mFzY3JpcHQ6Y2xvc2UoKTsi¶meters[3]=PiB8IDwvYT4iO30%3D)

http://tfa-dostmann.de/fileadmin/-----Anleitungen-----/98.1038_multi.pdf

