CENTRO 2030 Os Fundos Europeus mais próximos de si. PORTUGAL 2030 Cofinanciado pela União Europeia
estga universidade de aveiro

Fundamentos de Redes de Comunicação

CTESP – Redes e Sistemas Informáticos

10 – Debug

António Godinho

Sumário

- Técnicas de depuração de erros
- Ferramentas de depuração de erros

Motivação

- Administrador da rede é frequentemente chamado a resolver problemas de falha dos sistemas:
  - Sistemas falham (falha hardware, por intervenção humana, por causa de outros sistemas)
  - Redes possuem grandes quantidades de sistemas que dependem uns dos outros
  - Organizações necessitam de sistemas informáticos para produção
  - Utilizadores não sabem nem querem saber
    - "Não há rede!" ou "o servidor não funciona.."
  - e contam convosco para resolver ….

Contexto

- Resposta tem que ser célere
- Vai existir pressão
  - "ainda demora muito?"
  - "a facturação não consegue lançar vendas…"
  - "telefonou o Sr. …"

Como resolver

- Depuração é uma tecnica que melhora com experiência.
- Alguns aspectos que ajudam:
  - Isolar hipóteses
    - Dividir problema
  - Causa-efeito
    - Necessário corrigir a causa, não os efeitos
  - Ordem no processo de depuração
  - Persistência
  - Leitura das mensagens de erro
  - Fix once
    - Chanatisses vão dar problemas novamente!
  - Documentação de erros, sintomas e soluções

Restrição do problema

- Dividir para reinar:
  - Redes podem ter dezenas, centenas ou milhares de elementos
  - Determinar causa de problema em sistema de grandes dimensões é muito difícil
- Procurar reduzir domínio de forma a ter menos hipóteses de erro:
  - Testar coisas em separado de forma a eliminar hipóteses
  - Usar elementos substitutos e que funcionam
    - E.g.: se proxy não dá serviço ao browser usar telnet para porto do proxy e perceber se telnet obtem serviço

Ordem no processo

- Tentativa de solução rápida de problema pode levar a tentativas inconsistentes de detecção de erro
- Causalidade permite direcção de testes de forma:
  - Determinar o que se encontra a funcionar bem.
  - a eliminar falsas hipóteses
  - Destinguir causas das consequências
- Uma vez verificado que determinada hipótese não se verifica testam-se outras.

Persistência

- Necessário persistir:
  - O que é fácil, qualquer pessoa consegue fazer.
  - Por vezes mais ninguém nos pode ajudar
  - Autonomia depende da persistência em resolver problemas
    - E é muito bem vista!
- Necessário também saber parar:
  - Cerebro necessita de descanso
  - Por vezes estamos a olhar para o problema e não estamos a ver
  - Uma pausa faz maravilhas
    - Por vezes basta sair do local de trabalho para descobrir solução

Leitura das mensagens de erro

- Sistemas fazem log de funcionamento, e especialmente de erros
- Verificação de erros detectados permitem receber pistas do que correu mal
- Análise deve começam pelos primeiros erros;
  - Erros seguintes costumam ser consequência dos primeiros
- Procura de na web com a mensagem de erro costuma levar a foruns onde se discutem mesmos problemas
  - Permite descobir o que não é solução
  - Por vezes permite descobrir a solução para problema

Resolver os problemas de vez

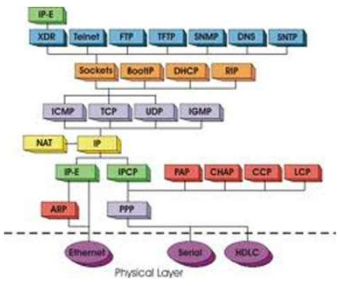
- Por vezes existe a tentação de arranjar uma solução temporária:
  - Coisas temporárias tornam-se definitivas
  - Esquecemos porque colocamos remendo
  - Outros administradores não percebem solução
  - Remendo vai criar problemas posteriores
- Fix once! Chanatisse dá sempre origem a problemas
- Exemplo: na falta de resolução de resolução de um nome podemos adicionar a tradução no hosts.Provavelmente vai lá ficar esquecida a tradução até ao dia em que essa tradução deixar de ser válida. Nesse dia vai ser uma confusão até se encontrar a entrada no hosts

Documentar problemas

- Problemas repetem-se
- Por vezes precisamos de horas ou dias para procurar causas
- Memória não guarda tudo; passados uma semana não resta muito
- Devemos documentar:
  - Causas de erro
  - Fontes de documentação
  - Soluções encontradas
  - Ferramentas de debug e correcção utilizadas
- Partilha de informação depende de organização:
  - Partilha entre administradores permite que conhecimento seja transmitido a quem estiver a trabalhar

Causa-efeito

- Modularidade da pilha protocolar faz com que as camadas superiores não funcionem sem terem serviço de camadas inferiores:
  - Sem conectividade não há endereço
  - Sem endereço não há resolução de nomes
  - Sem resolução de nomes browser não mostra conteúdo das páginas
  - Por onde começar?
- Sistemas dependem uns dos outros:
  - AD não funciona sem DNS
  - Email não funciona sem DNS
  - Erro detectado pode ser só a falha de email.
- Necessário ter em conta a dependência entre sistemas



13

Ferramentas de debug

Conectividade física

- Verificação de LED no concentrador e placa rede
- Windows mostra icon no systray
- UNIX tem ethtool (substituiu mii-tool
- Sintaxe:
  mii-tool [interface]

- arp permite verificar endereços MAC conhecidos
  root@comiander:~# arp -a
  Garlic.lan (192.168.1.65) at 68:a8:6d:53:ae:7e [ether] on eth0
  dsldevice.lan (192.168.1.254) at 08:76:ff:d0:6d:88 [ether] on eth0

Conectividade de rede

- **Ping**
  - Teste simples de conetividade
  - Envia pacotes ICPM ao destinatário e aguarda resposta medindo a percentagem de sucesso e tempo de resposta (*roud trip time*)

```
C:\Users\r>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=8ms TTL=64
Reply from 192.168.1.254: bytes=32 time=9ms TTL=64
Reply from 192.168.1.254: bytes=32 time=6ms TTL=64
Reply from 192.168.1.254: bytes=32 time=9ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 8ms
```


Conectividade de rede

- **Ping**
  - Caso de não resposta – não há conetividade – problemas de rede IP, switching ou cablagem!

```
C:\Users\r>ping 192.168.1.44

Pinging 192.168.1.44 with 32 bytes of data:
Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.

Ping statistics for 192.168.1.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

  - Se um ping ao endereço 127.0.0.1 der negativo, a placa de rede da máquina tem problemas!

Conectividade de rede

- **Ping**
  - Algumas opções importantes (cuidado que são diferentes em windows/linux):

ping –t -> pinga até fazermos ctrl+C
ping -n count -> envia a quantidade de pings indicada em count
ping -l size -> pinga através de pacotes de tamanho indicado em size – útil em certas aplicações

Identificação de máquina na rede

- arping efectua ping e apresenta o endereço MAC da máquina que responde

```
ARPING 192.168.39.120 from 192.168.39.1 eth0
Unicast reply from 192.168.39.120 [00:01:80:38:F7:4C]  0.810ms
Unicast reply from 192.168.39.120 [00:01:80:38:F7:4C]  0.607ms
Unicast reply from 192.168.39.120 [00:01:80:38:F7:4C]  0.602ms
Unicast reply from 192.168.39.120 [00:01:80:38:F7:4C]  0.606ms
Sent 4 probes (1 broadcast(s))
Received 4 response(s)
```

Consulta de rotas

- Falta de gw (rota para fora da rede) faz com que máquina não comunique com exterior da rede
- Falta de rota para destino faz com que router não reencaminhe pacote
- Equipamentos permite consultar tabelas de reencaminhamento:
  - Sintaxe em equipamentos linux
    route –n
  - Sintaxe em equipamentos windows
    route print
  - Sintaxe em equipamentos Cisco
    show ip route

Consulta de rota seguida por pacotes

- Pacotes são transmitidos passam por várias redes IP até chegarem ao destino
- Vários routers transpõem pacotes de rede para rede
- Cada pacote tem um TTL para evitar que em caso de perda ante eternamente na rede até chegar ao destino
- Cada router sempre que encaminham um pacote decrementa-lhe o TTL
- Quando TTL chega a 0 router descarta-o e manda mensagem ao originador a notificar.
- Envio sucessivo de pacotes com TTL crescente
  - permite receber mensagens de notificação de vários routers
  - Verificar por onde passam / param pacotes
  - Que elemento da rede está a atrasar as comunicações

traceroute

- **Traceroute**
  - Comando ***tracert*** em windows e ***traceroute*** em Linux;
  - Testa conetividade e acrescenta indicação do encaminhamento ao longo da rede permitindo descobrir o percurso e endereços IP dos Routers atravessados;

```
C:\Users\r>tracert 213.13.146.138

Tracing route to sapo.pt [213.13.146.138]
over a maximum of 30 hops:

  1    38 ms   121 ms    36 ms  speedtouch.lan [192.168.1.254]
  2     *        *         *     Request timed out.
  3   317 ms   617 ms    31 ms  b13-75-185.ds1.telepac.pt [213.13.75.185]
  4   232 ms   318 ms    78 ms  lcat1.v147.telepac.net [194.65.12.13]
  5   162 ms   303 ms   103 ms  lcat2.te1-1.telepac.net [213.13.135.150]
  6    27 ms    22 ms    21 ms  dial-b1-169-190.telepac.pt [194.65.169.190]
  7    25 ms    21 ms    28 ms  sapo.pt [213.13.146.138]

Trace complete.
```


traceroute

- **Traceroute**
  - Também permite a utilização de nome em vez do endereço IP desde que o DNS esteja a funcionar:

```
C:\Users\r>tracert www.sapo.pt

Tracing route to www.sapo.pt [213.13.146.138]
over a maximum of 30 hops:

  1     5 ms     7 ms     4 ms  speedtouch.lan [192.168.1.254]
  2     *        *        *     Request timed out.
  3    22 ms    24 ms    19 ms  b13-75-185.ds1.telepac.pt [213.13.75.185]
  4    34 ms    39 ms    27 ms  lcat1.v147.telepac.net [194.65.12.13]
  5    30 ms    30 ms    23 ms  lcat2.te1-1.telepac.net [213.13.135.150]
  6    24 ms    22 ms    21 ms  dial-b1-169-190.telepac.pt [194.65.169.190]
  7    29 ms    21 ms    23 ms  sapo.pt [213.13.146.138]

Trace complete.
```

  - O comando é útil para descobrirmos um ponto da rede com problemas ou a descobrir a própria constituição da rede.

traceroute

- **MTR** (My traceroute) – Só em Linux!
  - Combina informação do ping e traceroute e disponibiliza estatísticas:

```
                                My traceroute  [v0.82]
dax.prolixium.com (0.0.0.0)                                  Sun Jan  1 12:58:02 2012
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                 Packets               Pings
 Host                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. voxel.prolixium.net                         0.0%    13    0.4   1.7   0.4  10.4   3.2
 2. 0.ae2.tsr1.lga5.us.voxel.net                0.0%    12   10.8   2.9   0.2  10.8   4.3
 3. 0.ae59.tsr1.lga3.us.voxel.net               0.0%    12    0.4   1.7   0.4  16.0   4.5
 4. rtr.loss.net.internet2.edu                  0.0%    12    4.8   7.4   0.3  41.8  15.4
 5. 64.57.21.210                                0.0%    12    5.4  15.7   5.3 126.7  35.0
 6. nox1sumgw1-vl-530-nox-mit.nox.org           0.0%    12  109.5  60.6  23.0 219.5  66.0
    [MPLS: Lbl 172832 Exp 0 S 1 TTL 1]
 7. nox1sumgw1-peer--207-210-142-234.nox.org    0.0%    12   25.0  23.2  23.0  25.0   0.6
 8. B24-RTR-2-BACKBONE-2.MIT.EDU                0.0%    12   23.2  23.4  23.2  24.9   0.5
 9. MITNET.TRANTOR.CSAIL.MIT.EDU                0.0%    12   23.4  23.4  23.3  23.5   0.1
10. trantor.helicon.csail.mit.edu               0.0%    12   23.7  25.0  23.5  26.5   1.3
11. zermatt.csail.mit.edu                       0.0%    12   23.1  23.1  23.1  23.3   0.1
```

  - Para windows existe um programa: WinMTR

Resolução de nomes

- Maioria dos sistemas depende de DNS
- Nslookup procura tradução de nomes e endereços
- Sintaxe:

nslookup {nome|endereço} [servidor_nomes]

- Devolve nome quando se dá endereço; endereço quando se dá nome
- Não definição de servidor traduz-se em consulta ao resolver
- Resolver começa por verificar hosts
  - e.g.: /etc/hosts
- Depois passa para servidores de nomes listados na configuração do resolver
  - e.g.: /etc/resolver.conf

Serviço de nomes

- Procura de servidor primário
  nslookup -type=SOA ua.pt
- Procura de servidor de mail
  nslookup -type=mx ua.pt
- Procura de servidor de dns
  nslookup -type=ns ua.pt

```
nslookup -type=SOA ua.pt
Server:                 192.168.1.254
Address:        192.168.1.254#53
Non-authoritative answer:
ua.pt
        origin = ns.ua.pt
        mail addr = dns.cic.ua.pt
        serial = 496
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 86400

Authoritative answers can be found from:
ua.pt           nameserver = ns.ua.pt.
ua.pt           nameserver = ns2.ua.pt.
ns.ua.pt        internet address = 193.136.172.18
ns2.ua.pt       internet address = 193.136.172.19
```


Detecção de sessões abertas no sistema

```
root@comiander:~# netstat -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 comiander.local:ssh     Garlic.lan:55095        ESTABLISHED 1907/0
tcp        0      0 comiander.local:33092   none:1887               ESTABLISHED 1039/amuled
tcp        0      0 comiander.local:36959   static-174-255-224:4662 ESTABLISHED 1039/amuled
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
unix  7      [ ]         DGRAM                    3384     987/rsyslogd        /dev/log
unix  2      [ ]         DGRAM                    1876     245/udevd           @/org/kernel/udev/udevd
unix  3      [ ]         STREAM     CONNECTED     6658     2739/LaserJet%20101
unix  3      [ ]         STREAM     CONNECTED     6657     2738/HP_LaserJet_10
unix  3      [ ]         STREAM     CONNECTED     5060     1273/dbus-daemon    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     5059     1911/console-kit-da
unix  3      [ ]         STREAM     CONNECTED     5035     1273/dbus-daemon    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     5034     1911/console-kit-da
```

Portos abertos no sistema

```
root@comiander:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.1.2:4712        0.0.0.0:*               LISTEN      1039/amuled
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      1472/sshd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      786/portmap
tcp        0      0 0.0.0.0:51413           0.0.0.0:*               LISTEN      1529/transmission-d
tcp        0      0 192.168.1.2:53          0.0.0.0:*               LISTEN      1056/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1056/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1472/sshd
tcp        0      0 0.0.0.0:4662            0.0.0.0:*               LISTEN      1039/amuled
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN      1528/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1521/exim4
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      1056/named
tcp        0      0 0.0.0.0:9091            0.0.0.0:*               LISTEN      1529/transmission-d
tcp        0      0 0.0.0.0:38310           0.0.0.0:*               LISTEN      801/rpc.statd
tcp        0      0 192.168.1.2:22          192.168.1.65:55095      ESTABLISHED 1907/0
tcp        0      0 192.168.1.2:33092       91.225.136.126:1887     ESTABLISHED 1039/amuled
tcp        0      0 192.168.1.2:36959       77.224.255.174:4662     ESTABLISHED 1039/amuled
tcp6       0      0 :::139                  :::*                    LISTEN      1556/smbd
tcp6       0      0 :::110                  :::*                    LISTEN      1472/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      1077/apache2
tcp6       0      0 :::51413                :::*                    LISTEN      1529/transmission-d
tcp6       0      0 :::53                   :::*                    LISTEN      1056/named
```


Portos abertos na rede

```
root@comiander:~# nmap 192.168.1.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2012-07-16 15:49 WEST
Interesting ports on 192.168.1.2:
Not shown: 990 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
4662/tcp open  edonkey
9091/tcp open  unknown
```

Interesting ports on Garlic.lan (192.168.1.65):
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
88/tcp open kerberos-sec
548/tcp open afp
MAC Address: 68:A8:6D:53:AE:7E (Unknown)

Interesting ports on anis.lan (192.168.1.68):
Not shown: 996 filtered ports
PORT STATE SERVICE
80/tcp open http
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
MAC Address: E8:39:DF:DD:D6:04 (Unknown)

Ferramentas para Troubleshooting

- Ferramenta **Netstat**
  - Útil para saber estado das ligações ativas numa máquina incluindo sessões e portas:

C:>netstat

```
C:\Users\r>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5354         RuiPC:49412            ESTABLISHED
  TCP    127.0.0.1:5354         RuiPC:49413            ESTABLISHED
  TCP    127.0.0.1:49412        RuiPC:5354             ESTABLISHED
  TCP    127.0.0.1:49413        RuiPC:5354             ESTABLISHED
  TCP    192.168.1.73:49168     msnbot-191-232-139-73:https  ESTABLISHED
  TCP    192.168.1.73:55849     213.13.26.148:https    CLOSE_WAIT
  TCP    192.168.1.73:55905     wl-in-f188:5228        ESTABLISHED
  TCP    192.168.1.73:56016     195-23-85-126:8497     ESTABLISHED
  TCP    192.168.1.73:57158     ec2-23-21-77-157:https  CLOSE_WAIT
  TCP    192.168.1.73:57221     meocloud:http          ESTABLISHED
  TCP    192.168.1.73:57245     213.13.26.149:https    ESTABLISHED
  TCP    192.168.1.73:57246     213.13.26.149:https    ESTABLISHED
  TCP    192.168.1.73:57247     213.13.26.149:https    ESTABLISHED
  TCP    192.168.1.73:57248     84.39.153.33:http      CLOSE_WAIT
```


Verificar largura de banda

- iperf
  - Usa par cliente-servidor
  - Permite verificar LB em TCP e UDP
  - Aplicação comporta-se como um cliente ou como servidor dependendo de argumento de entrada
- Cliente

  iperf –c endereço servidor
- Servidor

  iperfc -s

Análise de uma máquina

```
root@comiander:~# nmap -P0 -A 192.168.1.68
Starting Nmap 5.00 ( http://nmap.org ) at 2012-07-17 18:17 WEST
Interesting ports on anis.lan (192.168.1.68):
Not shown: 996 filtered ports
PORT    STATE SERVICE      VERSION
80/tcp  open  http?
139/tcp open  netbios-ssn
443/tcp open  skype2       Skype
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: E8:39:DF:DD:D6:04  (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows XP|2000|2003 (93%)
Aggressive OS guesses: Microsoft Windows XP SP2 (93%), Microsoft Windows XP SP2 or SP3 (93%), Microsoft Windows XP SP2 (firewall disabled) (89%), Microsoft Windows
2000 SP4 or Windows XP SP2 or SP3 (88%), Microsoft Windows 2003 Small Business Server (88%), Microsoft Windows XP Professional SP2 (88%), Microsoft Windows XP SP3
(88%), Microsoft Windows Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP0 or Windows XP SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows
Host script results:
|_ nbstat: NetBIOS name: ANIS, NetBIOS user: <unknown>, NetBIOS MAC: e8:39:df:dd:d6:04
|  smb-os-discovery: Windows XP
|  LAN Manager: Windows 2000 LAN Manager
|  Name: SPICIES\ANIS
|_ System time: 2012-07-17 18:17:56 UTC+1
```


Acesso a serviço

- telnet abre uma sessão TCP com máquina destino.
- Permite verificar se servidor responde.
- Procedimento:
  - Abrir sessão no endereço e porto
  - Criar o diálogo usando o protocolo
- Pedido de conteúdo a proxy:

telnet proxy.ua.pt 3128

WGET http://www.dn.pt

- Outros exemplos: IMAP, POP, …..

Problemas causados por má configuração de DHCP

- Estações ficam completamente reféns de servidor de DHCP
  - Estações usam configuração do primeiro OFFER recebido
    - Pode ser uma **poisoned offer**
  - Não fazem ideia se servidor que enviou oferta está habilitado
    - Pode ser **rogue DHCP server**
  - Offer envenenado pode:
    - Fazer com que máquina fique sem serviço
    - Redireccionar tráfego para máquina que intermeie a comunicação.
      - Proxy – pelo WPAD
      - NAT – pelo router
      - DNS – pelo name server
- Detectar responsável
  - Windows – ipconfig /all
  - Linux - less /var/lib/dhcp3/dhclient.leases

Capturar tráfego de rede

- Wireshark ferramenta óptima e de utilização intuitiva
- tcpdump ferramenta em linha de comando que captura e mostra tráfego
- Permite gravar a captura para posterior visualização no wireshark
- Exemplos:

  tcpdump host sundown –w ficheiro

  tcpdump –i eth0 ip and not udp

- Mais info:

  man tcpdump

Fim

- Dúvidas?
- Comentários?