Toyota Network - Internal to APEagers

2011-07-04
Michael Spence

Audience:

Currently this document is primarily for use by the Systems Administrator for APEagers. It may be useful as a guide for the maintenance of this system by any other staff involved. It is assumed that the user of this guide, understands the use of services such as DNS, route tables, and packet filtering and basic networking paradigms.

Preamble:

The Toyota Extranet Network is connected to the APEagers WAN via two connections - one at EMP and one in Darwin.

This document describes what measures have been put in place to maintain a functional Toyota Network for the Toyota dealership we have under our control.

Specific only to Toyota: This document describes firewall configurations. This document describes proxy exceptions. This document describes the physical/logical layout of the network.

This document DOES NOT describe the firewall, proxies or network, where it is not in relation to Toyota.

Topics of Discussion

tSupport – Toyota Australia's Service Desk

Toyota Australia maintain their own Service Desk for Toyota related problems. Their contact details are:

Phone	1800 251 175
Email	tsupport@toyota.com.au

Topics in Detail

1. DAN Router

Each Toyota (in a perfect Toyota world) is supplied with an ADSL modem and Router (often combined) which connects directly to the Toyota network for their state. Through this connection the Toyota and TMCA networks are accessible.

Servicing QLD and NT are two DAN routers for the current six (6) Toyota locaions under APEagers control. One DAN router is housed at the APEagers Data Centre at Eight Mile plains and the other at the Darwin Network Core at Bridge Toyota Darwin City.

The IP addresses for the DAN routers are as follows:

EMP DAN Router	10.40.1.46
DWN DAN Router	172.16.1.8

See the latest recorded copy of the DAN configuration for the EMP DAN Router in Topic 7.

1.1 Access Lists

The DAN routers have been configured to allow only specific subnets of the WAN to access the Toyota/TMCA networks. The subnets allowed are listed below:

EMP DAN Router

```
10.1.0.0/16
10.5.0.0/16
10.18.0.0/16
10.25.0.0/16
10.32.0.0/16
10.51.0.0/16
```

DWN DAN Router

```
10.50.0.0/16
10.51.0.0/16
```

1.2 NEC Contacts

Administration for the DAN routers is performed by NEC. At this time, there is only limited, contact details for these contractors.

Victor Teh

Email	Victor.Teh@nec.com.au
Phone	03 9262 1037
Mobile	0411 658 407

2. Toyota Destinations

The Toyota Extranet network is known quite well and it can be easily confirmed that the following subnets describe parts of the Toyota Extranet.

Toyota Subnets

```
10.9.100.0/24
132.147.0.0/16
150.45.0.0/16
192.168.42.0/24
192.168.101.0/24
192.168.108.0/24
192.168.109.0/24
129.168.206.0/24
```

3. Firewall Configurations

For PC access from the WAN the firewall must be configured to route traffic destined for the Toyota Extranet through the DAN router.

The following routes are configured to be started at firewall startup:

Firewall configuration file rc.local extract

```
route –n add –net 10.9.100.0/24 10.40.1.46
route –n add –net 132.147.0.0/16 10.40.1.46
route –n add –net 150.45.0.0/16 10.40.1.46
route –n add –net 192.168.42.0/24 10.40.1.46
route –n add –net 192.168.101.0/24 10.40.1.46
route –n add –net 192.168.108.0/24 10.40.1.46
route –n add –net 192.168.109.0/24 10.40.1.46
route –n add –net 192.168.206.0/24 10.40.1.46
```

Also for PC's to access these networks, the packet filter must also allow traffic to traverse to these networks without the aid of a proxy. The following PF rules are configured to allow traffic through the firewall and consequently through the DAN router.

Firewall configuration file pf.conf extract

```
sites_toyota = "10.9.100.0/24, 132.147.0.0/16, 150.45.0.0/16,
                  192.168.42.0/24, 192.168.101.0/24, 192.168.108.0/24,
                  192.168.109.0/24, 192.168.206.0/24, 208.39.44.0/24,
                  208.39.45.0/24, 216.14.206.48"
table <proxy_bypass> const { $sites_toyta, ... et al }
pass in quick on $int_if proto { tcp, udp } \
            from any to <proxy_bypass> port { 80, 443 }
```

4. DNS configurations

Domain resolution cannot be done across the internet for *.toyota.com.au and *.tmca.com.au as these are not generally accessible internet destinations. Due to this DNS servers which are located in the Toyota Extranet must be used. The two DNS servers provided to use are:

```
192.168.109.38
192.168.109.138
```

To facilitate this DNS functionality within our own network, our DNS servers use DNS forwarding for the name resolution of toyota.com.au and tmca.com.au domains.

5. Proxy Configuratons

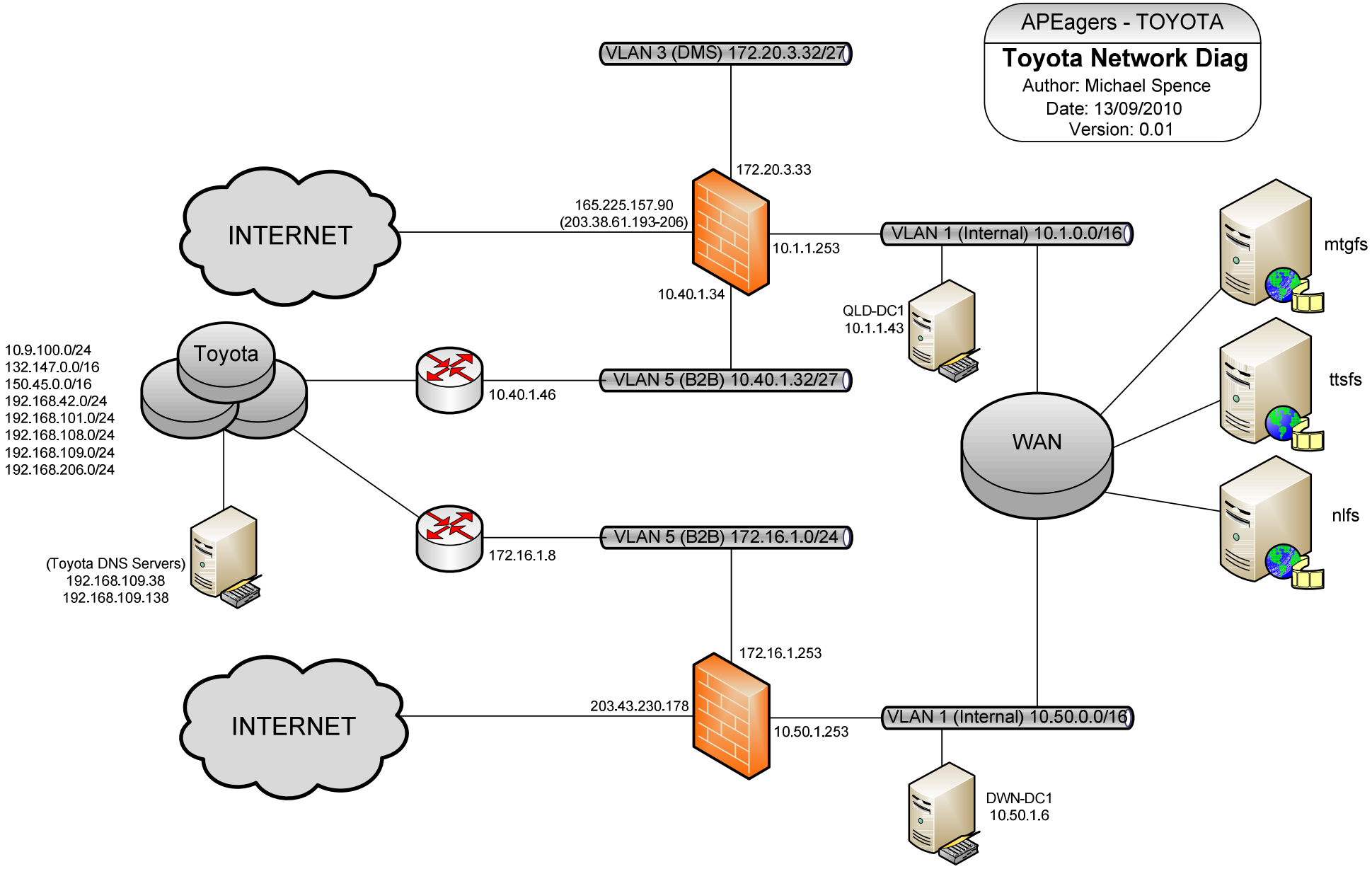
Almost all Toyota traffic is allowed through the firewall and onto the Toyota Extranet. As such there is no need for a proxy to access Toyota sites contained on the Extranet. However, a proxy is required to gain Internet access. Due to this requirement the following Proxy Exceptions are required for Toyota Users:

Extract of proxy exceptions as seen in IE

```
*.tmca.com.au
*webapps.toyota.com.au
tjunction.toyota.com.au*
*.partner.toyota.com.au
150.45.156.*
```

6. Physical/Logical Layout

The following image describes the Logical layout of our network. PCs and users exist generally within the WAN and the firewalls maintained are at EMP and DWN.


APEagers - TOYOTA
Toyota Network Diag
Author: Michael Spence
Date: 13/09/2010
Version: 0.01
VLAN 3 (DMS) 172.20.3.32/27
172.20.3.33
INTERNET
165.225.157.90
(203.38.61.193-206)
10.1.1.253
VLAN 1 (Internal) 10.1.0.0/16
10.40.1.34
QLD-DC1
10.1.1.43
mtgfs
ttsfs
nlfs
10.9.100.0/24
132.147.0.0/16
150.45.0.0/16
192.168.42.0/24
192.168.101.0/24
192.168.108.0/24
192.168.109.0/24
192.168.206.0/24
Toyota
10.40.1.46
VLAN 5 (B2B) 10.40.1.32/27
WAN
(Toyota DNS Servers)
192.168.109.38
192.168.109.138
172.16.1.8
VLAN 5 (B2B) 172.16.1.0/24
172.16.1.253
INTERNET
203.43.230.178
10.50.1.253
VLAN 1 (Internal) 10.50.0.0/16
DWN-DC1
10.50.1.6

7. DAN Router Configuration (as at 2009-07-31)

```
version 12.4
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TDQEMP0C0878
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
enable secret 5 $1$IRat$pSwL/68ZFyStLmxVSrSqv1
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authentication login no_tacacs local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
!
!
aaa session-id common
clock timezone GMT+10 10
clock summer-time EDST recurring last Sun Oct 2:00 last Sun Mar 3:00
!
crypto pki trustpoint TP-self-signed-1207741901
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1207741901
 revocation-check none
 rsakeypair TP-self-signed-1207741901
!
!
crypto pki certificate chain TP-self-signed-1207741901
 certificate self-signed 01
  30820253 308201BC A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31323037 37343139 3031301E 170D3032 30333031 30303036
  34315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 32303737
  34313930 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100E3F0 CAF6572D 03C888AA B5AFEF5F 40F1222F BFE86F50 C253E7AC DB5160BE
  E3E081E5 A47CA9C1 93E4E40E 4F88A183 C80DC7CA 10204944 C4FEFF59 C277C76A
  1C8FC181 F94ADE06 D5183D6B 0AC5B025 CC2BCD8C A6EB85E1 1D18C029 8ED8BC0B
  FD553C08 A064EB89 64F9C002 8E91DFBD 0ED26E82 C1981274 17A380C0 3183ADC2
  200F0203 010001A3 7B307930 0F060355 1D130101 FF040530 030101FF 30260603
  551D1104 1F301D82 1B544451 454D5030 43303837 382E796F 7572646F 6D61696E
  2E636F6D 301F0603 551D2304 18301680 14CD48CE A8236C09 2A08AAD6 8FE20B89
  B726E0B5 CC301D06 03551D0E 04160414 CD48CEA8 236C092A 08AAD68F E20B89B7
  26E0B5CC 300D0609 2A864886 F70D0101 04050003 8181009B 5C26BFEB B65F0766
  38C1D1BE 02EACD24 11BA23BA 01D84282 5F52EEED 596CC4C4 A5AA4BA5 B43CDA55
  FDEACE6D 08A4E19C FEC85D42 814F8C62 CC6C070A 29AA9DD6 DD04C9C8 F2D3CA68
  0892170E C9590835 76F20AF1 033A1845 396F7628 38A7F1CF E2F05754 6DED5A37
  596AEBFC 4730DD10 6D062DC8 4CA874CC 6BDFE864 8EB836
       quit
dot11 syslog
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1
```

```
!
ip dhcp pool sdm-pool
   import all
   network 10.10.10.0 255.255.255.248
   default-router 10.10.10.1
   lease 0 2
!
!
no ip domain lookup
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
vtp mode transparent
username necaretoyota privilege 15 secret 5 $1$r8un$ww0jxL/sPH414.kk5.GaU/
username cisco privilege 15 secret 5 $1$B6BD$D6C/xqImPmVpv6GOpJTw4/
!
!
archive
 log config
  hidekeys
!
!
controller DSL 0
 mode atm
 line-term cpe
 line-mode auto enhanced
 dsl-mode shdsl symmetric annex B
!
vlan 1000
 name NEXTEP-DEALER-LAN
!
!
class-map match-all GOLD_SERVICE
 match access-group name GOLD_TRAFFIC
class-map match-all BRONZE_SERVICE
 match access-group name BRONZE_TRAFFIC
class-map match-all SILVER_SERVICE
 match access-group name SILVER_TRAFFIC
class-map match-all DEFAULT_SERVICE
 match access-group name DEFAULT_TRAFFIC
!
!
policy-map DAN_QoS_Policy_Ver1.0_10-11-2008
 class GOLD_SERVICE
  bandwidth percent 50
 class SILVER_SERVICE
  bandwidth percent 15
 class BRONZE_SERVICE
  bandwidth percent 10
 class DEFAULT_SERVICE
  bandwidth percent 5
!
!
!
!
interface Loopback0
 description NEC Management Interface
 ip address 172.20.9.9 255.255.255.252
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface ATM0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
```

```
 ip flow ingress
 no atm ilmi-keepalive
 max-reserved-bandwidth 80
 service-policy output DAN_QoS_Policy_Ver1.0_10-11-2008
!
interface ATM0.1 point-to-point
 description *** Connection to NEC NEXTEP IP/VPN ***
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 snmp trap link-status
 pvc 0/33
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface FastEthernet0
 description *** Connection to TOYOTA Dealer LAN ***
 switchport access vlan 1000
!
interface FastEthernet1
 shutdown
!
interface FastEthernet2
 shutdown
!
interface FastEthernet3
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 ip address 10.40.1.46 255.255.255.0 secondary
 ip address 192.168.122.1 255.255.255.248
 ip mtu 1492
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
interface Dialer0
 ip address negotiated
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname sl01632w@ipvpn.nexnet.net.au
 ppp chap password 0 B0F4F529
!
ip forward-protocol nd
ip route 10.0.0.0 255.0.0.0 10.40.1.34
ip route 10.0.0.0 255.255.224.0 Dialer0
ip route 10.9.100.0 255.255.255.0 Dialer0
ip route 10.12.100.0 255.255.255.0 Dialer0
ip route 10.255.254.0 255.255.255.0 Dialer0
ip route 172.20.0.0 255.255.240.0 Dialer0
ip route 172.20.3.34 255.255.255.255 10.40.1.34
ip route 172.20.3.40 255.255.255.255 10.40.1.34
ip route 192.168.108.0 255.255.254.0 Dialer0
ip route 192.168.122.0 255.255.255.128 Null0
ip route 192.168.251.3 255.255.255.255 10.40.1.34
```

```
!
!
no ip http server
ip http access-class 23
no ip http secure-server
ip nat pool natpool 192.168.122.8 192.168.122.107 prefix-length 25
ip nat inside source list 21 pool natpool
ip nat inside source static 10.40.1.51 192.168.122.108
!
ip access-list extended BRONZE_TRAFFIC
 permit tcp any any eq domain
 permit tcp any eq domain any
 permit icmp any any
ip access-list extended DEFAULT_TRAFFIC
 permit ip any any
ip access-list extended GOLD_TRAFFIC
 permit tcp any any eq www
 permit tcp any eq www any
 permit tcp any eq 443 any
 permit tcp any any eq 443
 permit tcp any any eq telnet
 permit tcp any eq telnet any
 permit tcp any any range 3200 3650
 permit tcp any any range 4700 4850
 permit tcp any range 3200 3650 any
 permit tcp any range 4700 4850 any
 permit tcp any any eq 88
 permit tcp any eq 88 any
ip access-list extended SILVER_TRAFFIC
 permit tcp any any eq ftp
 permit tcp any eq ftp any
 permit tcp any any eq ftp-data
 permit tcp any eq ftp-data any
!
ip sla responder
access-list 21 permit 172.20.3.40
access-list 21 permit 172.20.3.34
access-list 21 permit 10.52.0.0 0.0.255.255
access-list 21 permit 10.40.1.0 0.0.0.255
access-list 21 permit 10.1.0.0 0.0.255.255
access-list 21 permit 172.20.3.0 0.0.0.255
access-list 21 permit 10.16.0.0 0.0.255.255
access-list 21 permit 10.22.0.0 0.0.255.255
access-list 21 permit 10.24.0.0 0.0.255.255
access-list 21 permit 10.25.0.0 0.0.255.255
access-list 21 permit 10.28.0.0 0.0.255.255
access-list 21 permit 10.5.0.0 0.0.255.255
access-list 21 permit 10.15.0.0 0.0.255.255
access-list 21 permit 10.18.0.0 0.0.255.255
access-list 21 permit 10.36.0.0 0.0.255.255
access-list 21 permit 10.33.0.0 0.0.255.255
access-list 21 permit 10.34.0.0 0.0.255.255
access-list 21 permit 10.51.0.0 0.0.255.255
access-list 21 permit 10.1.1.0 0.0.0.255
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 60 remark - ACL FOR SNMP SOURCE FILTERING
access-list 60 permit 10.255.254.0 0.0.0.255
access-list 60 deny   any log
access-list 61 remark - ACL FOR TELNET SOURCE FILTERING
access-list 61 permit 10.255.254.0 0.0.0.255
access-list 61 permit 10.147.0.0 0.0.255.255
access-list 61 permit 132.147.0.0 0.0.255.255
access-list 61 permit 172.21.0.0 0.0.255.255
access-list 61 permit 192.168.0.0 0.0.255.255
access-list 61 deny   any log
dialer-list 1 protocol ip permit
snmp-server community NECpublic RO 60
snmp-server community NECprivate RW 60
snmp-server location "Toyota DAN - Southside Toyota Eight Mile Plains QLD "
snmp-server chassis-id TDQEMP0C0878
no cdp run
```

```
!
!
!
tacacs-server host 10.255.254.18
tacacs-server directed-request
tacacs-server key 7 02120A5E08071D2442431A
!
control-plane
!
banner exec ^CC
**************************************************************
Toyota site : Southside Toyota Eight Mile Plains QLD
This is a NEC NEXTEP IP/VPN network. It has special
configuration requirements. Do not change.
**************************************************************
^C
banner motd ^CC
**************************************************************************
                                WARNING

Access to this system is for NEC authorised users and for
authorised purposes only.

Unauthorised access or use is a serious breach of NECs security policies,
and may constitute a criminal or civil offence. If you or your intended use
are not authorised do not proceed to log onto this system.
**************************************************************************
^C
!
line con 0
 exec-timeout 30 0
 login authentication no_tacacs
 no modem enable
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 30 0
 privilege level 15
 transport input telnet ssh
!
scheduler max-task-time 5000
ntp authentication-key 123 md5 030A0808125E2C1F 7
ntp authenticate
ntp trusted-key 123
ntp clock-period 17175026
ntp source Loopback0
ntp server 10.255.254.240
end
```