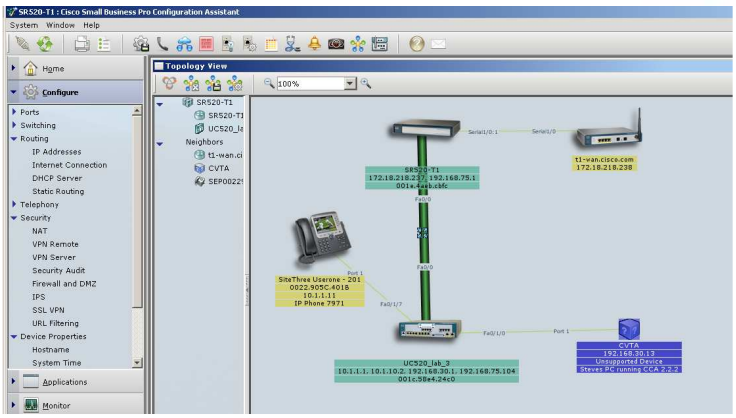
Cisco Small Business Pro

Smart Business Communication System

Technical Enablement Labs



Lab 15

Cisco SR 520-T1 Secure Router

(can be 'head end' Security Router for a UC 500)

Introduction

This document allows the reader to see how easy it is to implement a SR 520-T1 Secure Router in the small business environment with T1 Data WAN interconnect requirements. It can also be used as an internal lab you can perform on your own to become familiar and comfortable with this product. Lastly, it helps concierge the reader through the process of taking one out of the box and finding everything one needs to deploy it. This is not a substitute for on line Administrative Guides, Smart Designs, QSGs, or the like. Sometimes seeing a deployment document helps bring everything together in an understandable way.

The nice part about this setup, is it requires no CLI. Running the SR-520-T1 Configuration Utility, which is embedded inside CCA (as well as being offered inside the code zip file on CCO for SR520-T1) is all you need to get the router up and running and then it can be managed (configuration) from Cisco Configuration Assistant (CCA).

I would like to add that the capacity of a T1 interface is one we would expect to see at a host (Main) campus location, so while the SR520-Ethernet and DSL interface routers (cousins to the T1 model) are recommended for remote teleworker purposes, the SR520-T1 is not. It can be implemented as a head end security router for the UC500. In my deployment, I will be using it as the head end security router for a UC500 which is part of a 5 site multisite mesh, which means it is fully supported by CCA Multisite Manager as well.

Preparing for SR520-T1 Initial Configuration

The SR520-T1 datasheet shows 3 diagrams of the supported SR520-T1 topologies and uses where a small business needs to interconnect to a T1 Data WAN.

This document will address the basic WAN interconnect and setup.

The figures are cut and pasted right from the datasheet.

Figure 2. Cisco SR 520-T1 Secure Router Data Deployment

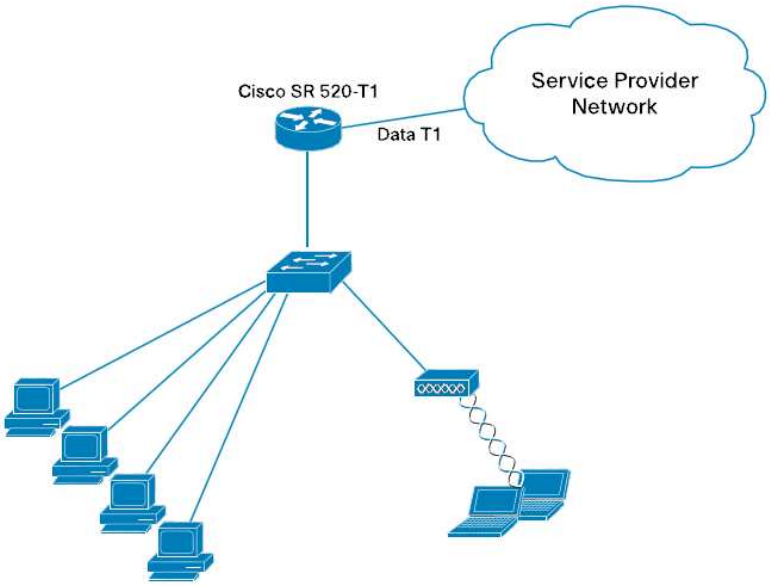


Figure 3. Cisco SR 520-T1 Secure Router Deployment as Part of the Cisco SBCS

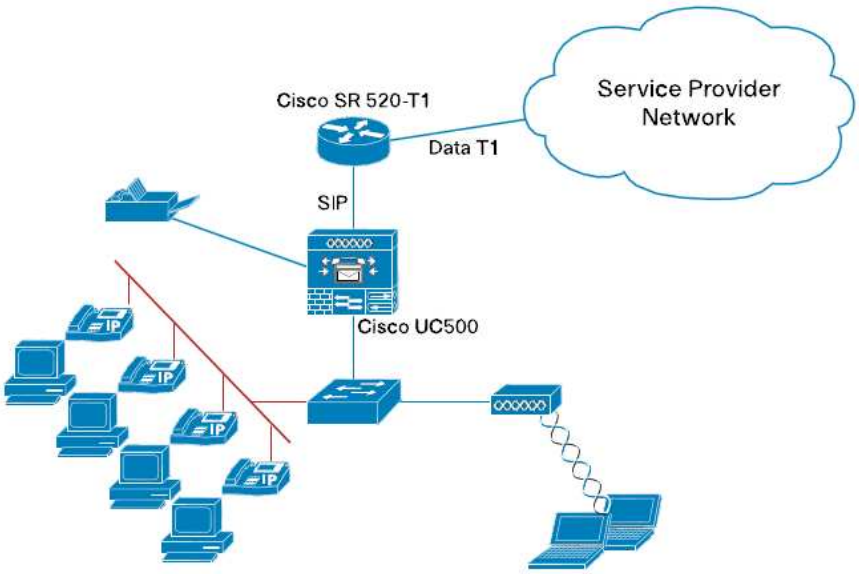
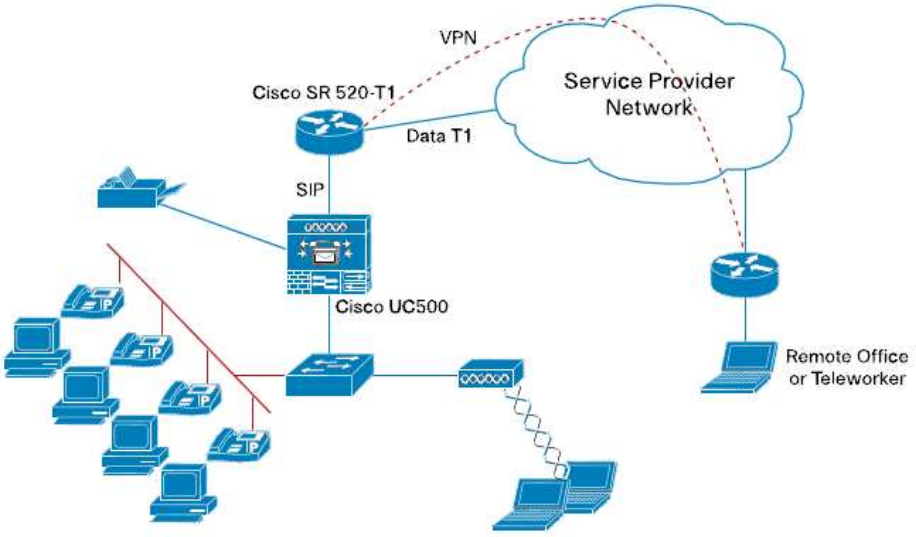


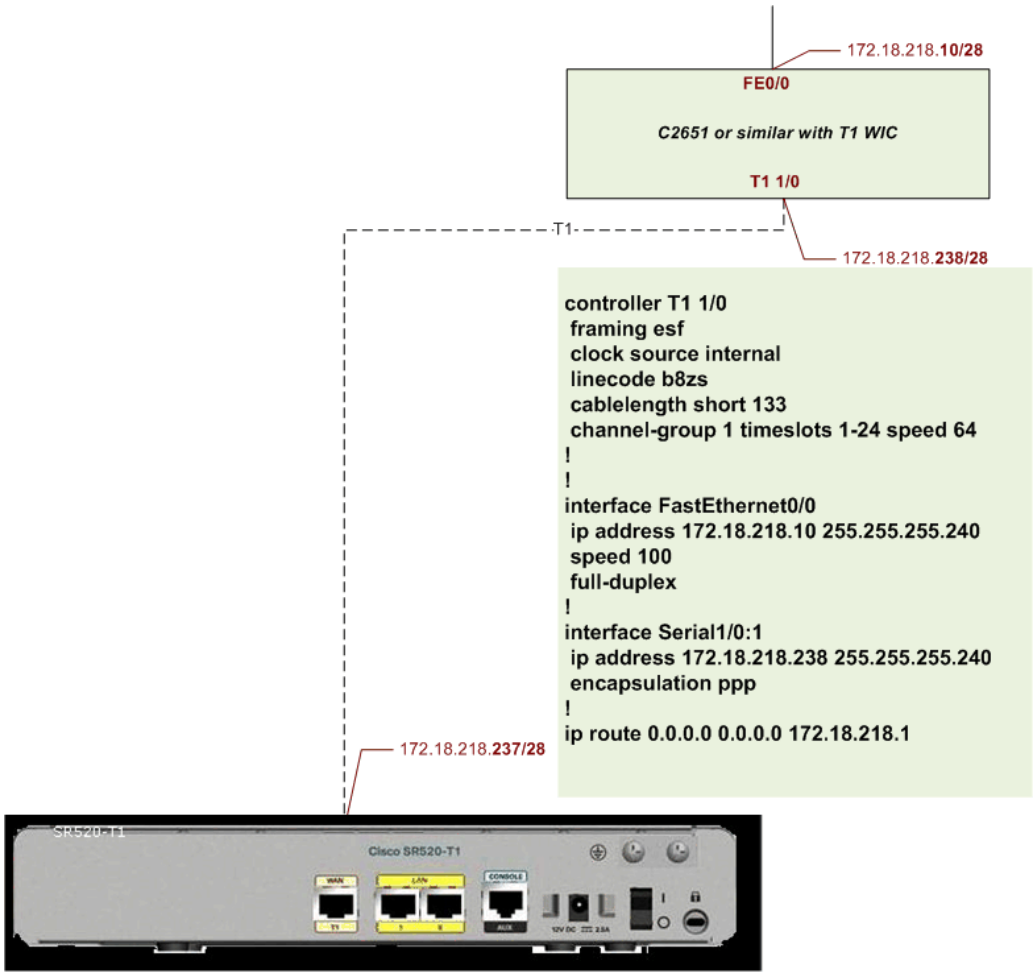
Figure 4. Cisco SR 520-T1 Secure Router Site-to-Site / Teleworker VPN Deployment



Determine the T1 Router Connection and Configuration

In my case, since I don't have a Data T1 from a real Service Provider terminating in my lab, I used an internal lab 2651 with a T1 WIC. It connects to the "lab net" (a simulated internet) on it's FE port and the T1 extends to my SR520-T1. The SR520 can connect directly to the Data T1 of the S.P., and this lab is only that (a lab).

The important thing to note here is T1 attributes like encapsulation, Line Code and Frame Format, and number of channels supported (fractional or full) and mach the configuration on the SR520-T1 side with that of the Service Provider's T1.



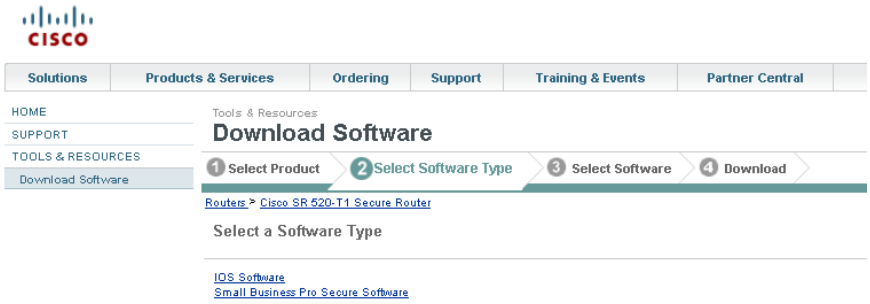
Note: The 2651 T1 Router configuration (show run) is in the Appendix

Software/Firmware for the SR520-T1

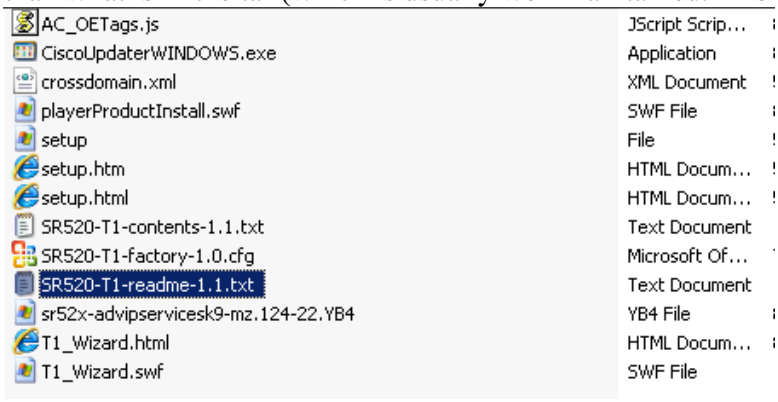
This step may not be needed, depending on when the SR520-T1 was shipped from the factory to Distribution, since it usually ships with the latest FW.

Where to Find the Firmware:

www.cisco.com/go/sr500
There is a .tar file under Small Business Pro Secure SW link, which includes the IOS FW plus other components. Download it.



You can refer back to the IOS Software link only if advised that you need a newer IOS than what is in the tar (which is usually well maintained. Here is a view of that tar file:

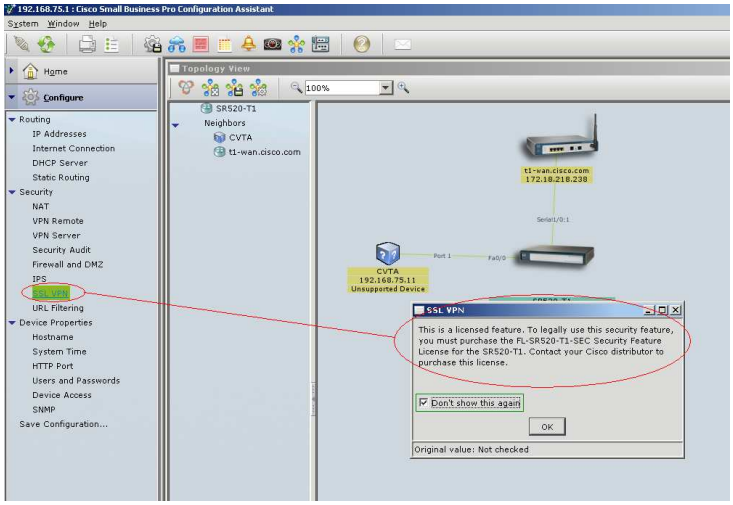


Licenses required for some functions on the SR520-T1

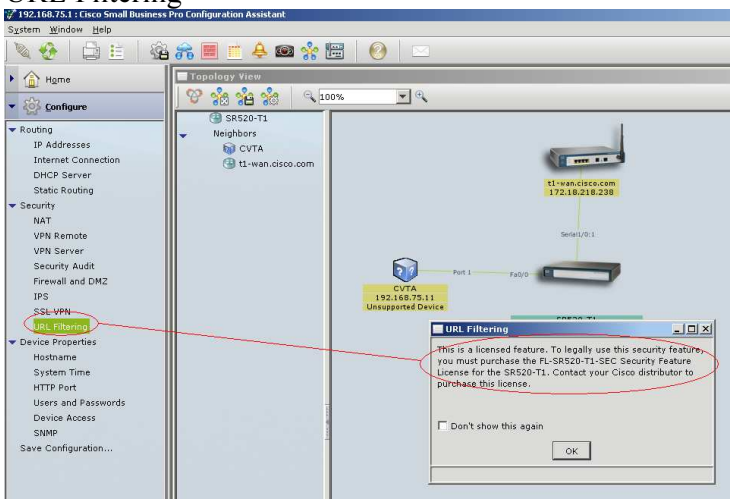
You may want to have your License SKUs ready at this point since some configuration capability will require them (shown below)

FL-SR520-T1-SEC

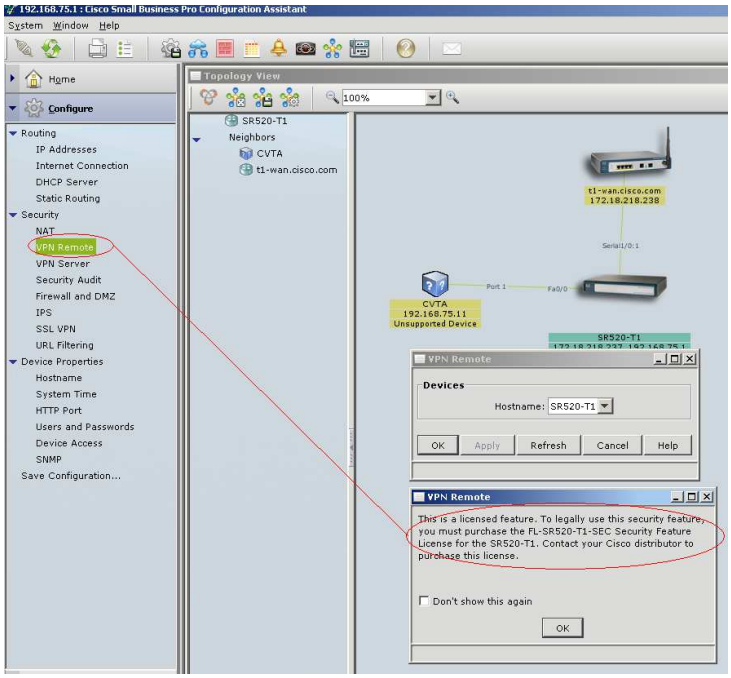
SSL VPN



URL Filtering



VPN Remote



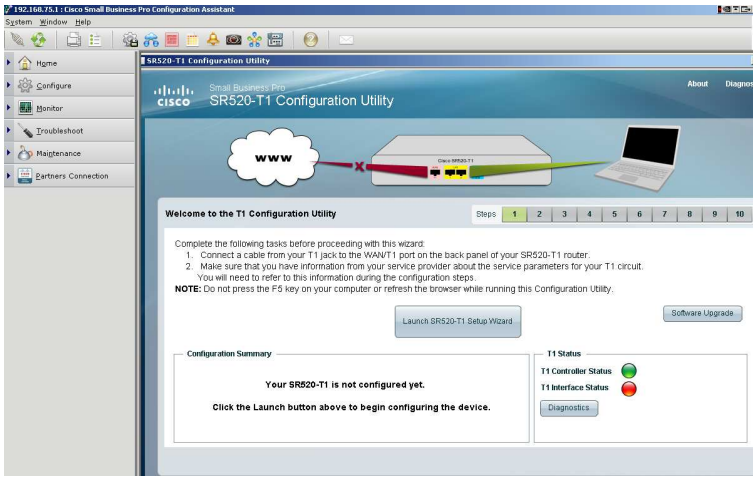
CCA Configuration of the SR520-T1

Connect your PC running CCA to Port 0 on the SR520 LAN connector, and the T1 cable from your Internet router to the T1 connector on the SR520-T1.

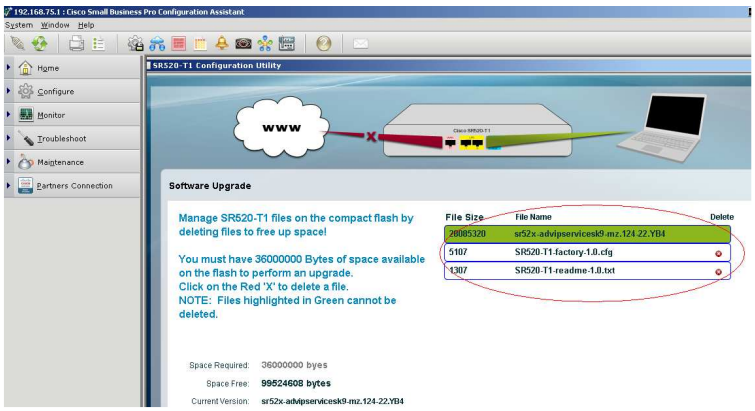
CCA T1 Configuration Utility

Launch CCA (Latest Release; this done on CCA 2.2.2) and point at 192.168.75.1 (cisco/cisco is default UID/PW). CCA will launch the SR520-T1 configuration utility.

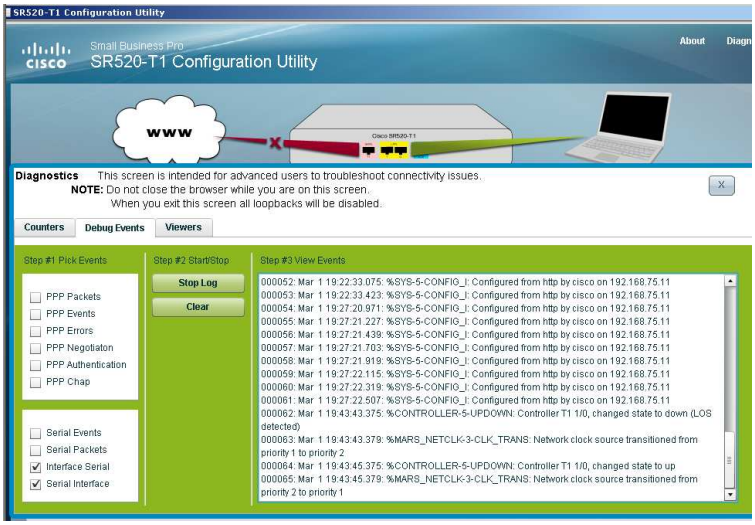
Step 1 – Check the Firmware and Diagnostics



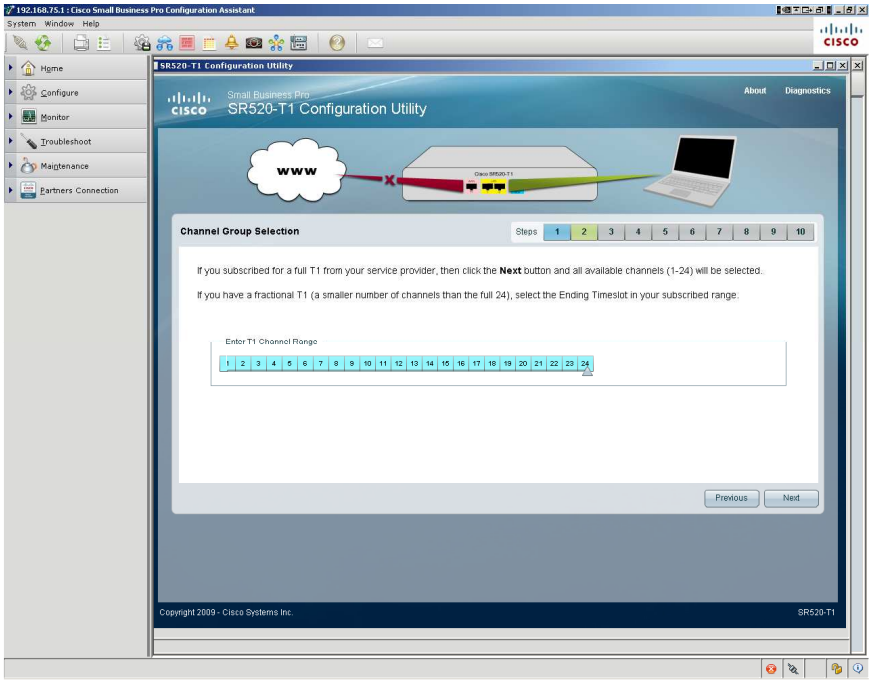
Check the FW level of the unit by clicking “Software Upgrade” and then “Manage Files on Flash”. Below mine is the same as what is on CCO:



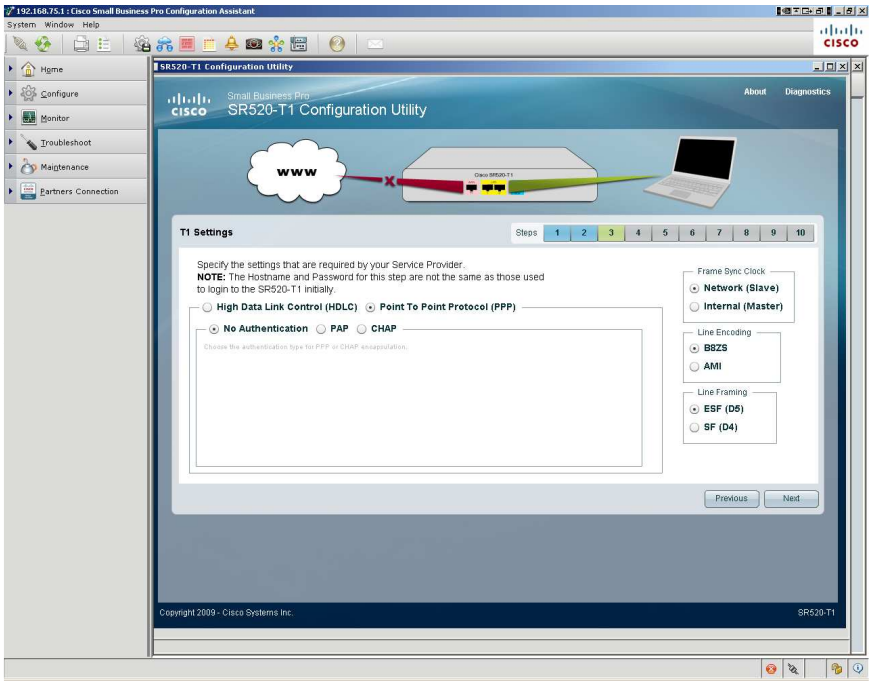
Check the diagnostics when you plug in your T1. Since you haven’t configured the SR520, you can expect to see only physical layer connectivity at this point (why the Link to the www cloud is Red).



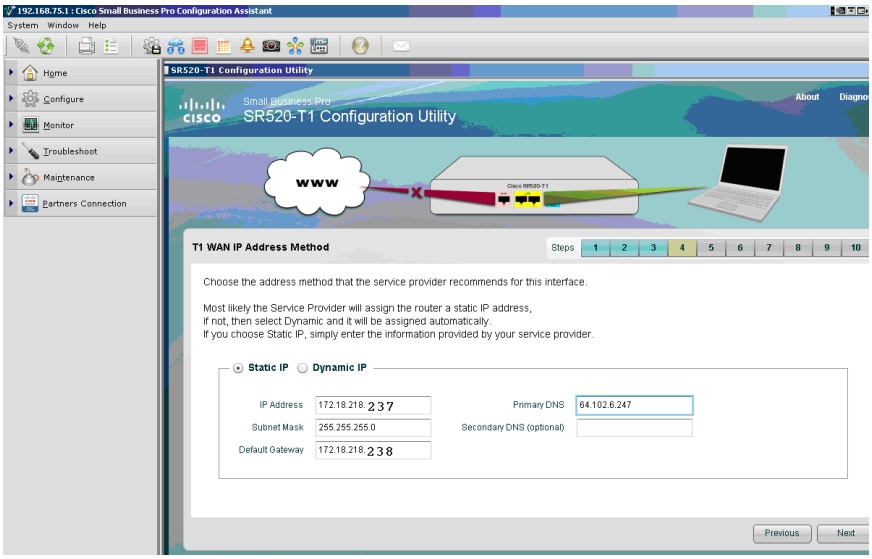
Step 2 – Define the number of DS0s to be used



Step 3 – T1 Settings



Step 4 – IP Addressing

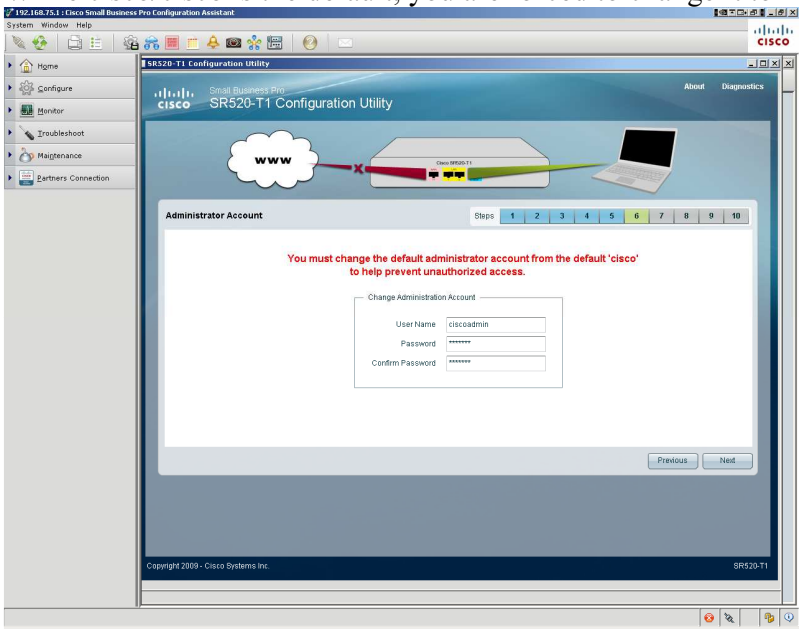


Step 5 - Confirm

Confirm what you set so far and click next.

Step 6 – Adjust the User/Pass

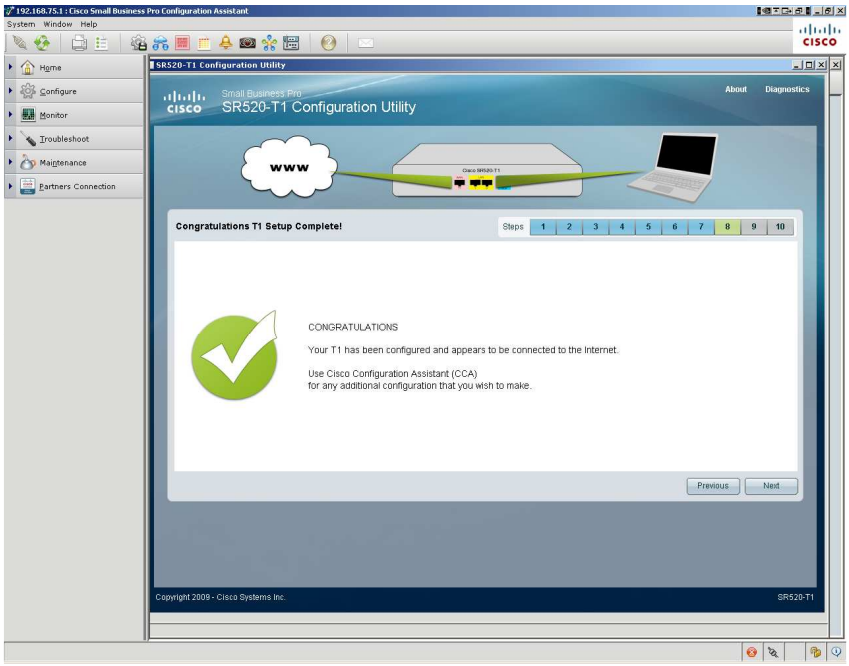
While cisco/cisco is the default, you are forced to change it to more than 6 characters.



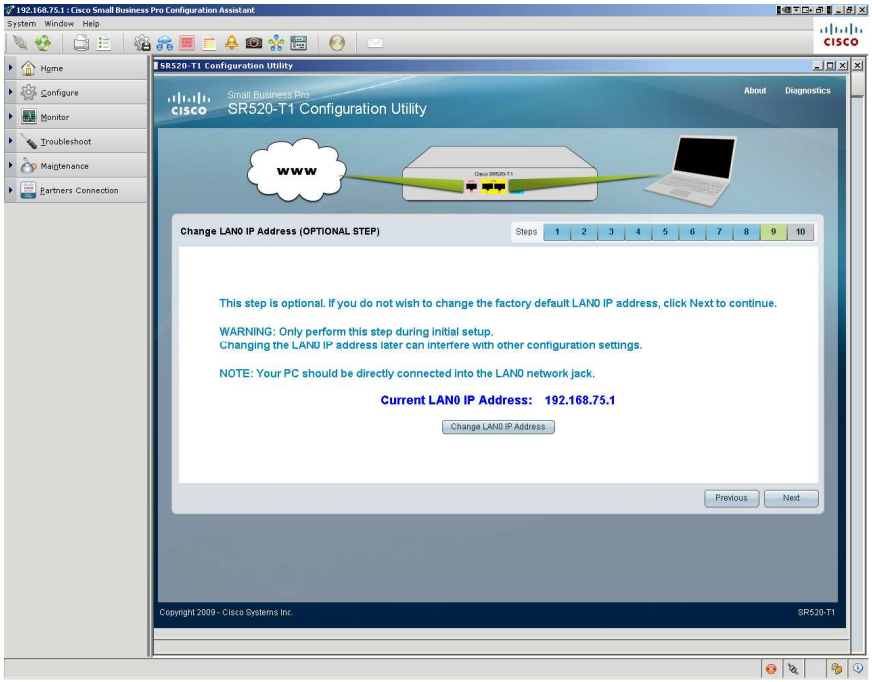
Step 7 - APPLY

Apply the settings. Notice when done, the T1 Interface becomes routable and usable, therefore green:

Step 8 - Congratulations



Step 9 – Optional LAN IP

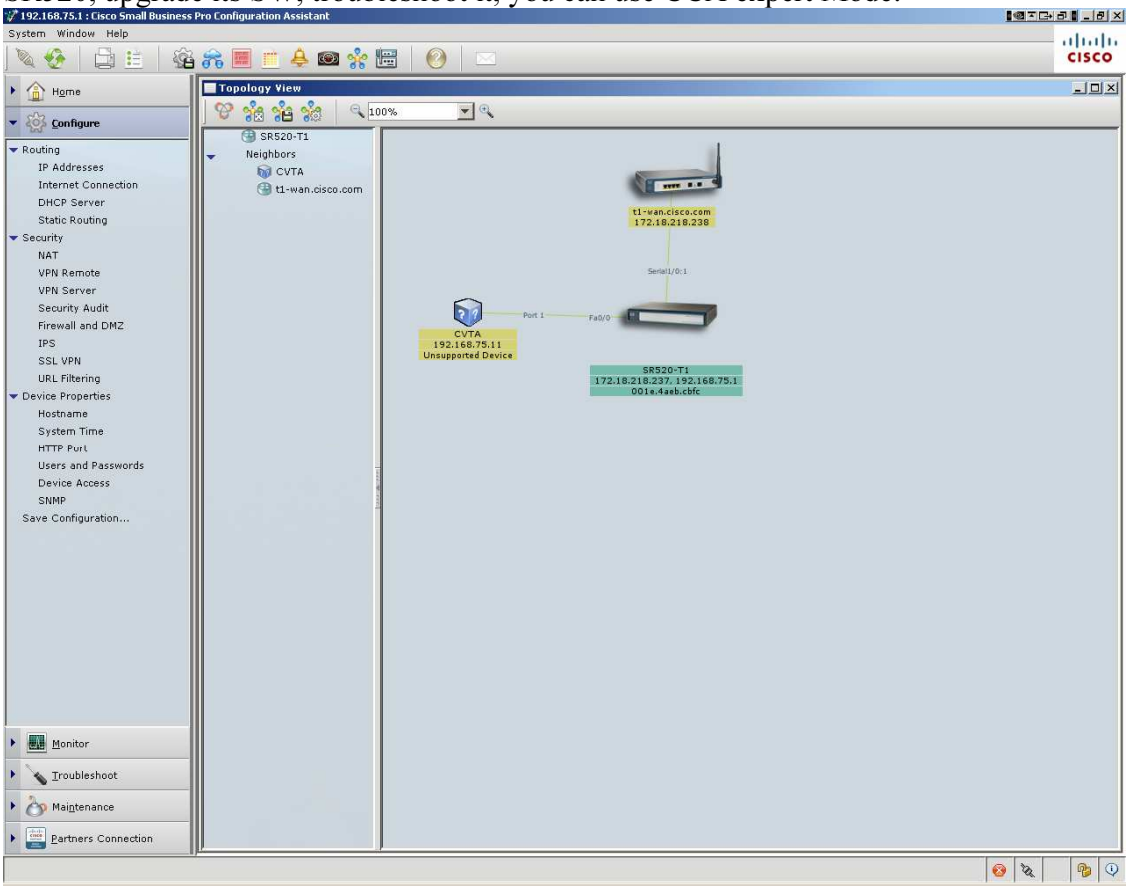


Step 10 - Finish

Click Next and Finish

CCA Expert Mode

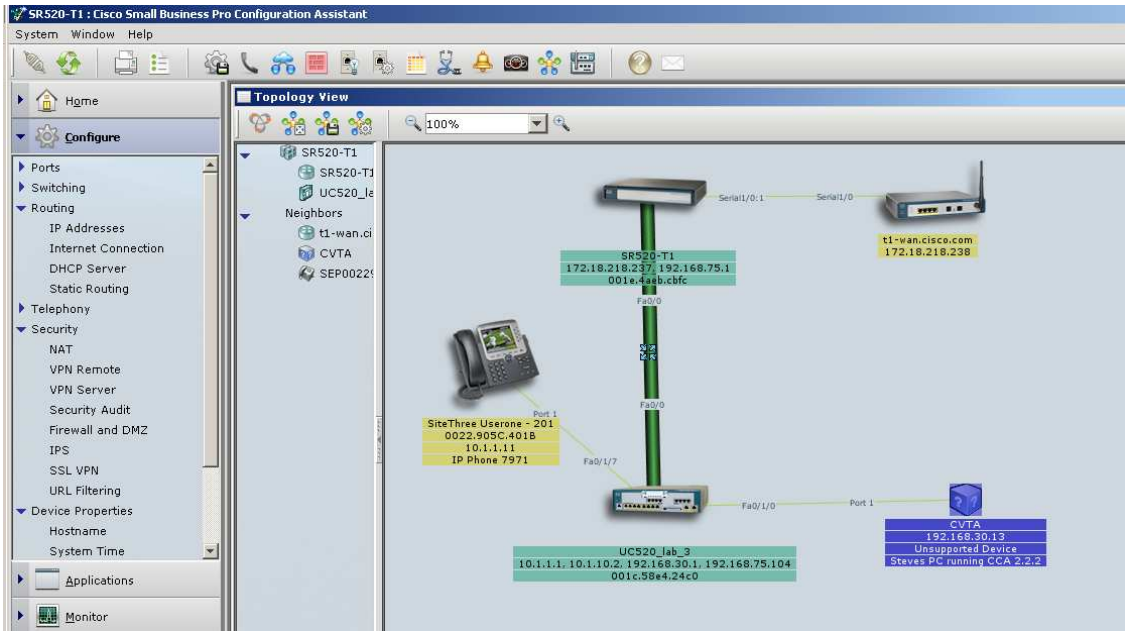
If you made any configuration errors or later need to change something, monitor the SR520, upgrade its SW, troubleshoot it, you can use CCA expert Mode.



After you do an ipconfig /release and /renew, your client PC can now be connected to the WWW.

I have since added this SR520-T1 as the head end Security Router for one of my UC500s (UC520-lab-3) which is a member of a 5 site Multisite in my lab. I configured this completely with CLI as well, and the CCA MSM detected the SR520-T1 and accommodated it into the configuration as well.

Here is how it looks in CCA, where I discovered the SR520 and then it detected the Neighbors, and I 'added to community' the UC520-lab-3.



Now the SR520-T1 and the UC520 and both managed from the same instance of CCA (version 2.2.2 in my case)

Caveat

I fond one small problem in my deployment. The 172.18.218.0/24 is an internal Cisco Lab network, which can wee our Intranet. So when my PC is connected behind any of the UC520s in the multisite, it can connect to the intranet. I found that site 3 (UC520-lab-3) for which this SR520-T1 sits in front of, was not able to connect.

After a few times trying to debug this, I came to realize that the SR520-T1 ACL 104 was missing one statement that when added manually, allowed the PC to connect through the SR520-T1 to Cisco Intranet. I was assured by the BU, that CCA would have placed that statement and I must have done something to remove that and maybe they are right, as this is a lab after all. But I list in anyway, in case you ever have a similar problem:
This is what my SR-520-T1 system showed for ACL 104….

```
access-list 104 remark SDM_ACL Category=2
access-list 104 deny   ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 104 deny   ip 192.168.75.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 104 deny   ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 104 deny   ip 192.168.75.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 104 deny   ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 104 deny   ip 192.168.75.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 104 deny   ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 104 deny   ip 192.168.75.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 104 permit ip 192.168.75.0 0.0.0.255 any
```

I added " access-list 104 permit ip 192.168.30.0 0.0.0.255 any"

Appendix

Included are:

- T1-WAN Internet Router Configuration
- SR520-T1 CLI Running Configuration

T1-WAN Router (2651) running configuration:

```
t1-wan#sh run
Building configuration...
Current configuration : 1561 bytes
! Last configuration change at 11:56:19 EST Tue Feb 9 2010
version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname t1-wan
!
boot-start-marker
boot-end-marker
!
logging buffered 1000000 debugging
no logging console
enable secret 5 $1$1KXi$wipN0GBwOAKvuBJbEC2bc.
enable password cisco
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
clock summer-time EDT recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
voice-card 1
!
ip cef
!
no ip domain lookup
ip domain name cisco.com
ip name-server 64.102.6.247
isdn switch-type primary-ni
!
!
controller T1 1/0
```

```
 framing esf
 clock source internal
 linecode b8zs
 cablelength short 133
 channel-group 1 timeslots 1-24 speed 64
!
interface FastEthernet0/0
 ip address 172.18.218.10 255.255.255.240
 speed 100
 full-duplex
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:1
 ip address 172.18.218.238 255.255.255.240
 encapsulation ppp
!
ip route 0.0.0.0 0.0.0.0 172.18.218.1
ip route 192.168.75.0 255.255.255.0 172.18.218.237
!
no ip http server
no ip http secure-server
!
control-plane
!
no mgcp package-capability res-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input all
!
ntp clock-period 17208207
ntp server 172.18.108.15
!
end
```

SR520-T1 Running Configuration (result of CCA Wizard)

```
SR520-T1#sh run
Building configuration...

Current configuration : 6936 bytes
!
! Last configuration change at 15:00:54 PST Fri Mar 1 2002 by ciscoadmin
! NVRAM config last updated at 13:35:19 PST Fri Mar 1 2002 by ciscoadmin
!
version 12.4
parser config cache interface
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
service sequence-numbers
!
hostname SR520-T1
!
boot-start-marker
boot-end-marker
!
card type t1 1
logging message-counter syslog
logging buffered 1024000
no logging console
no logging monitor
enable secret 5 $1$5mXb$klotPe69WdgHJWsZQx4H5.
!
no aaa new-model
clock timezone PST -8
clock summer-time PST recurring
network-clock-participate T1 1/0
network-clock-select 1 T1 1/0
!
crypto pki trustpoint TP-self-signed-4176713398
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4176713398
 revocation-check none
 rsakeypair TP-self-signed-4176713398
!
!
crypto pki certificate chain TP-self-signed-4176713398
```

```
 certificate self-signed 01
  30820240 308201A9 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34313736 37313333 3938301E 170D3032 30333031 30303038
  34335A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 31373637
  31333339 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  81009FC9 2386E7C7 0AC88429 90434ABA 7B9ABE34 F2AB1E4E 7751273E
FDD2C62A
  6280324B FC877FFB CD839AB1 38E8DE03 94B53BAA 35A4A1A2 B598294A
587B69B8
  11E8911E 5C7C2808 D19AB49F 79BB7D49 E4355436 55F5B6BD 28BC827B
3045F930
  F6FD28A6 B308C382 ECC14B24 8DDA9557 DA288E69 45DF7A75 C1B216B1
868E964F
  158B0203 010001A3 68306630 0F060355 1D130101 FF040530 030101FF 30130603
  551D1104 0C300A82 08535235 32302D54 31301F06 03551D23 04183016 8014D288
  FF530F31 4846A530 A6DB68BB 4921E577 313D301D 0603551D 0E041604
14D288FF
  530F3148 46A530A6 DB68BB49 21E57731 3D300D06 092A8648 86F70D01
01040500
  03818100 936BD051 6BE9F1EE F62EA227 16232DEE CF071AE0 F8B12A75
C5670957
  B20431C4 23BFB12C DFB947CD E53870EA 1A80C784 318C2E7D D1592EC4
CD2EB523
  AFE116B8 17657654 0B2FCCAD 14F80FAD 7598709B BF0A3C1F C73BAFF3
9BC42BD6
  7C67FDF4 5FBEA479 E97D6440 52EF8098 39226231 79DE4E80 8D399542
B1635E0B 0B0CAC
9F
       quit
ip source-route
!
!
ip dhcp relay information trust-all
ip dhcp excluded-address 192.168.75.1 192.168.75.10
!
ip dhcp pool data
   import all
   network 192.168.75.0 255.255.255.0
   default-router 192.168.75.1
   dns-server 64.102.6.247
!
!
ip cef
ip name-server 64.102.6.247
```

```
ip inspect log drop-pkt
no ipv6 cef
!
multilink bundle-name authenticated

parameter-map type inspect z1-z2-pmap
 audit-trail on
!
username ciscoadmin privilege 15 secret 5 $1$MxE1$pemcQOCSVsNtZcyhX6E3y/
!
!
!
archive
 log config
  logging enable
  logging size 600
  hidekeys
!
!
controller T1 1/0
 channel-group 1 timeslots 1-24
!
!
class-map type inspect match-any SDM-Voice-permit
 match protocol sip
class-map type inspect match-any sdm-cls-icmp-access
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-any sdm-cls-insp-traffic
 match protocol cuseeme
 match protocol dns
 match protocol ftp
 match protocol h323
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol netshow
 match protocol shell
 match protocol realmedia
 match protocol rtsp
 match protocol smtp extended
 match protocol sql-net
 match protocol streamworks
 match protocol tftp
```

```
 match protocol vdolive
 match protocol tcp
 match protocol udp
class-map type inspect match-all sdm-invalid-src
 match access-group 100
class-map type inspect match-all dhcp_out_self
 match access-group name dhcp-resp-permit
class-map type inspect match-all dhcp_self_out
 match access-group name dhcp-req-permit
class-map type inspect match-all sdm-protocol-http
 match protocol http
!
!
policy-map type inspect sdm-permit-icmpreply
 class type inspect dhcp_self_out
  pass
 class type inspect sdm-cls-icmp-access
  inspect
 class class-default
  pass
policy-map type inspect sdm-inspect
 class type inspect SDM-Voice-permit
  pass
 class type inspect sdm-cls-insp-traffic
  inspect
 class type inspect sdm-invalid-src
  drop log
 class type inspect sdm-protocol-http
  inspect z1-z2-pmap
 class class-default
  pass
policy-map type inspect sdm-inspect-voip-in
 class type inspect SDM-Voice-permit
  pass
 class class-default
  drop
policy-map type inspect sdm-permit
 class type inspect dhcp_out_self
  pass
 class class-default
  drop
!
zone security out-zone
zone security in-zone
zone-pair security sdm-zp-self-out source self destination out-zone
 service-policy type inspect sdm-permit-icmpreply
```

```
zone-pair security sdm-zp-out-in source out-zone destination in-zone
 service-policy type inspect sdm-inspect-voip-in
zone-pair security sdm-zp-out-self source out-zone destination self
 service-policy type inspect sdm-permit
zone-pair security sdm-zp-in-out source in-zone destination out-zone
 service-policy type inspect sdm-inspect
!
!
!
interface FastEthernet0/0
 description $FW_INSIDE$
 ip address 192.168.75.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security in-zone
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $FW_INSIDE$
 no ip address
 ip nat inside
 ip virtual-reassembly
 zone-member security in-zone
 duplex auto
 speed auto
!
interface Serial1/0:1
 description $FW_OUTSIDE$
 ip address 172.18.218.237 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 zone-member security out-zone
 encapsulation ppp
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.18.218.238
ip route 192.168.10.0 255.255.255.0 FastEthernet0/0
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:
ip nat inside source list 1 interface Serial1/0:1 overload
!
```

```
ip access-list extended dhcp-req-permit
 remark SDM_ACL Category=1
 permit udp any eq bootpc any eq bootps
ip access-list extended dhcp-resp-permit
 remark SDM_ACL Category=1
 permit udp any eq bootps any eq bootpc
!
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 192.168.75.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 permit 10.1.10.0 0.0.0.3
access-list 100 remark SDM_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 172.18.218.224 0.0.0.15 any
!
!
!
!
control-plane
!
!
!
!
banner login ^CSR520-T1 Configuration Utility. Version: 1.0  Cisco Configuration
 Assistant Tue Feb 9 2010^C
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login local
 transport input all
line vty 5 100
 login local
 transport input all
!
exception data-corruption buffer truncate
ntp master
end
```