APRICOT 2011 Hong Kong
Network Security Workshop

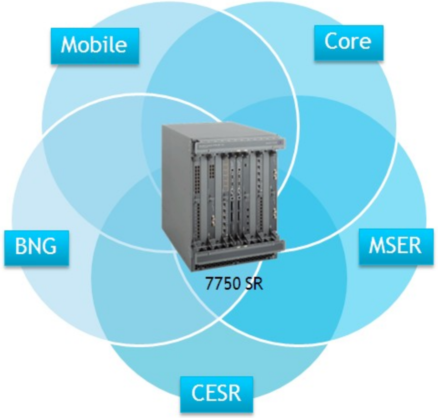
Alastair JOHNSONalastair.johnson@alcatel-lucent.com

Jonny MARTIN jonny@pch.net

Tony CHAN tonychan@juniper.net

15 February 2011

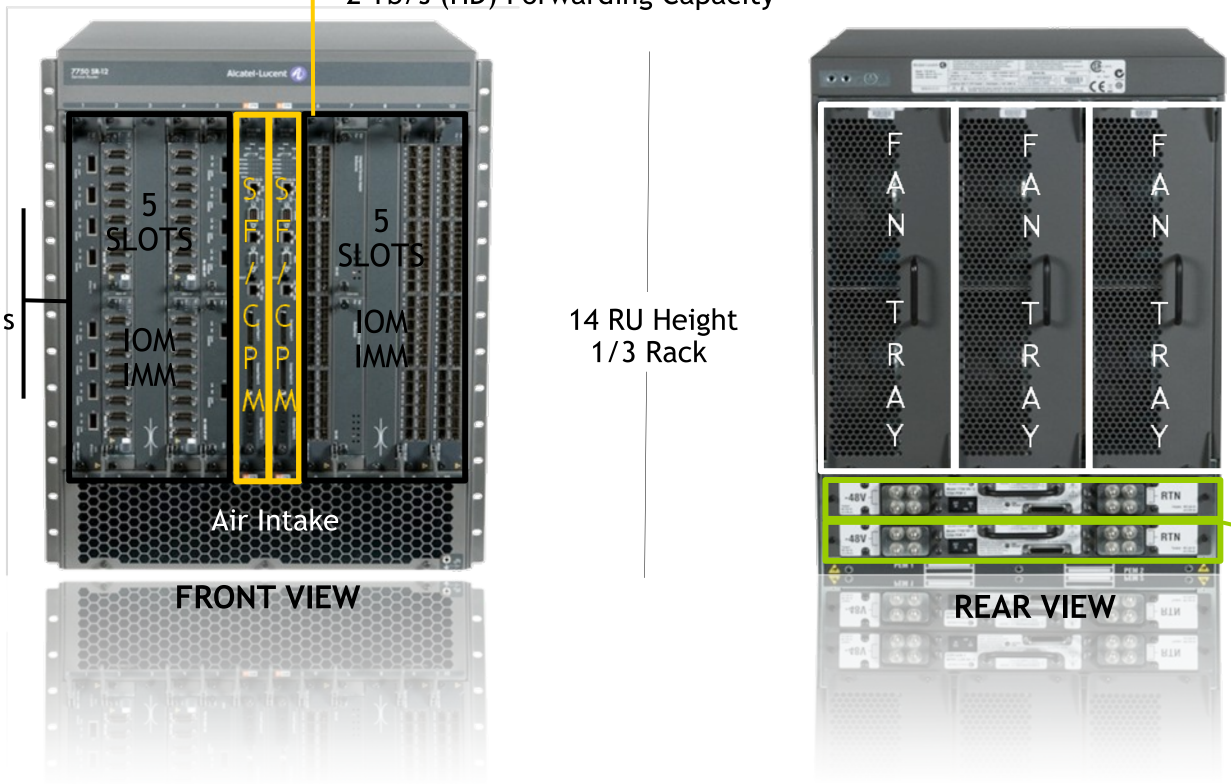
Advanced Platforms: The 7750 SR Product Family



7750 SR-12	7750 SR-7	7750 SR-c12	7750 SR-c4
2 Tb/s	1 Tb/s	90 Gb/s	90 Gb/s
12 slots (10 user slots) in 1/3 rack	7 slots (5 user slots) in 8RU	12 compact slots (or 3 full slots)	4 compact slots - fully front accessible
High Availability, ISSU	High Availability, ISSU	High Availability, ISSU	Red’t pwr & cooling
Terabit IP/MPLS multiservice router	Mid-scale IP/MPLS multiservice router	Small POP router for SPs & Verticals	Small POP router for business services edge

Four chassis variants in the 7750 SR family

Alcatel-Lucent 7750 SR-12 Chassis Overview



1+1 Switch Fabric/Control Processor Module with Redundancy (Dual Active Fabrics)

2 Tb/s (HD) Forwarding Capacity

19" Rack Width

10 Input/Output Line Card Slots with 20,50 or 100 Gb/s slots

14 RU Height
1/3 Rack

N+1 Cooling Redundancy

Front-to-back Airflow

NEBS3 compliant

1+1 DC Power Inputs

AC through external 1 RU rectifiers

High-end multi-service edge/core router

Alcatel-Lucent 7710 SR-c4 Architecture

Physical

- 3 RU Height: 13.3 cm (5.3 in.)
- Width: 44.4 cm (17.5 in.)
- Depth: 55.9 cm (22.0 in.)

18 Gbps (HD) CFM (Control and Forwarding Module)

Modular Design

- 4 horizontal slots for interfaces
- Up to four Compact Media Adapter (CMAs)
- Up to two Media Dependent Adapters (MDAs)
- . . . Or combination of both
- Aggregation down to DS1/E1

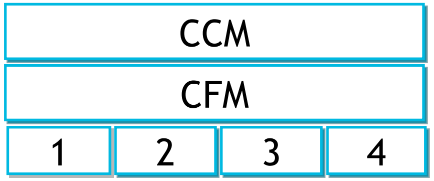
System Redundancy

- Power modules and fans

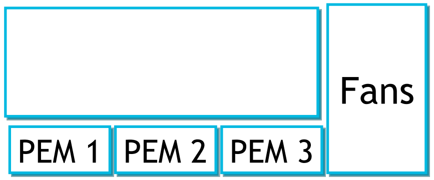
Leverages Flexible Fast Path Technology

- Highly scalable packet processing, advanced traffic management, and high-touch service capabilities.
- No lengthy ASIC spin cycles for new feature implementation

Front View



Rear View



Chassis Control Module (CCM)
Control & Forwarding Module (CFM)
Power Entry Module (PEM)

Router Components

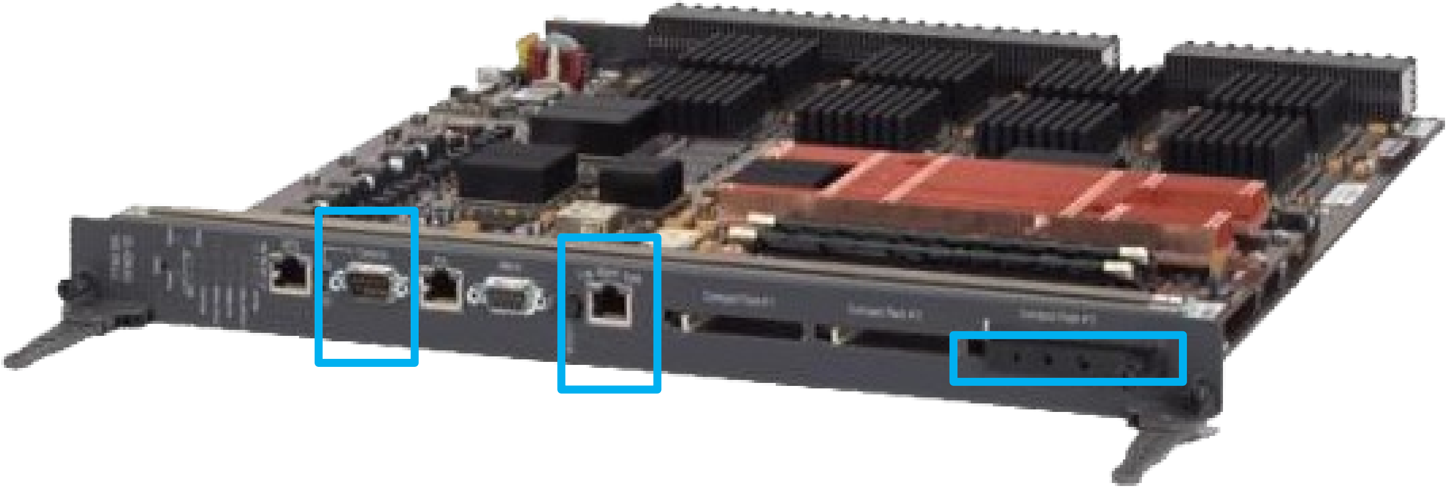
- **BOF – Boot Options File – defines the configuration for router bootstrap (config, software, etc) and out-of-band configuration.**
- POST – Power On Self Test – checks for basic functionality of router hardware and determines what interfaces are present.
- RAM – holds the running software, routing memory, packet buffers, etc. There are multiple types of RAM in the 7750SR present on multiple cards.
- Flash – holds the software, log files, and persistent configuration. There are three flash slots in the 7750SR (per SF/CPM).
- **SF/CPM – Switch Fabric/Control Plane Module, that provides the switch fabric between slots and the control processor that runs the main SR-OS software and centralised functions like routing protocols.**
- **IOM – I/O Module that provides connectivity to MDAs and the switch fabric, hosts the queuing and packet forwarding functions.**
- **MDA – Media Dependent Adapter hosted in an IOM, and provides the physical layer connectivity.**

In the lab

- Two 7750SR-12
  - Redundant SF/CPM3
  - IOM3-XP
  - 10-port Gigabit Ethernet MDA-XP
- Two 7710SR-c4
  - Single CFM
  - 1-port Gigabit Ethernet CMA
- Slot / Card / Port starting at 1.
  - 1/1/1 is the Workshop Gigabit Ethernet port in use.

Access Router's Management Ports

- Console
  - DB9 EIA-232 @ **115200bps**, 8/N/1 (pre-configured)
- Management Port, using telnet or SSH
  - Requires configuration



Alcatel·Lucent

Initial Login - SROS

```
TiMOS-B-8.0.R5 both/hops ALCATEL SR 7710 Copyright (c) 2000-2010
Alcatel-Lucent.

All rights reserved. All use subject to applicable license
agreements.

Built on Tue Sep 28 18:27:04 PDT 2010 by builder in
/rel8.0/b1/R5/panos/main



Login: admin

Password: admin

*A:NS065051303#
```

EMAC Style Shortcuts

Shortcut	Key Combination
Start of Line	Ctrl-A (^A)
End of Line	Ctrl-E (^E)
Delete Line	Ctrl-U (^U)
Delete Cursor to End of Line	Ctrl-K (^K)
Delete Previous Word	Ctrl-W (^W)
Redraw Line	Ctrl-L (^L)
Exit from config mode	Ctrl-Z (^Z)

Command Completion

- Space bar completes a command
- Tab key completes a variable
  - But not all of them!
- \ can be used to run a top-level command from any context
  - `config>router>service#\show time`
- Help is available with ? after any command

```
A:NS065051303# configure service
  - service


 [no] apipe           + Provision an ATM-Pipe Service
 [no] cpipe           + Provision a Circuit Emulation Pipe Service
 [no] customer        + Provision a customer
 [no] egress-multica* + Create an Egress Multicast Group
 [no] epipe           + Provision an Ether-Pipe Service
[…]
```

Using | (Pipe)

- The pipe function is used to filter output
  - Available in some modes and context

```
- match <pattern> context {parents|children|all} [ignore-case] [max-count
  <lines-count>] [expression]
- match <pattern> [ignore-case] [invert-match] [pre-lines <pre-lines>]
  [post-lines <lines-count>] [max-count <lines-count>] [expression]

<pattern>              : string or regular expression
<pre-lines>            : [0..100]
<lines-count>          : [1..2147483647]
```

Router Modes Change and Prompts

- A:Router#
  - Default privileged mode at the root prompt.
  - ‘A’ refers to the SF/CPM
  - ‘Router’ is the hostname
- A:Router>config#
  - Configuration mode
- A:Router>config>service#
  - Sub-context within configuration mode
- A:Router>config>service>vprn$
  - Newly created context
- *A:Router#
  - Config has been changed **and is unsaved**

Key CLI commands

- show
  - Applicable to most things: ports, cards, interfaces, routing table, services, etc.
  - The **detail** keyword is often very useful.
- admin
  - Admin commands such as upgrade, save, reboot, time setting, etc.
- tools
  - Debugging and OAM tools that run on the router
- configure
  - Enter configuration mode. You can append full configure statements to this, e.g. ‘configure port 1/1/1 ethernet speed 1000’
- monitor
  - Port/SAP/service/etc monitor commands
- And many more. Start with ‘?’ !

Router and Service Constructs

- Router refers to the base routing instance
  - This is the backbone configuration for the router, mostly used for forming routing adjacencies between other PE and P routers.
  - All MPLS, BGP, OSPF, IS-IS, etc configuration is performed here.
  - Ports must be configured for **network** mode.
- Services are configured under the **service** construct
  - VLL = EPIPE, IPIPE, APIPE, FPIPE, CPIPE
  - VPLS = VPLS
  - VPRN = Virtual Private Routed Network (VRF)
  - IES = Internet Enhanced Service, **use this for Internet Routing Services**
- Services are associated with **customers** – this is mostly a billing construct, and we can use a single customer ID for the workshop.
- Services must be configured on **access** ports.

Router and Service Constructs

- Services have Service Access Points (SAP)
  - These are logical interfaces within the service, that are associated to a port.
  - The interface name does not have to be the same as the port name.
  - E.g: `interface “jonny” sap 1/2/3:4` refers to an interface called ‘jonny’ on physical port 1/2/3, sub-interface 4.
  - For consistency, I like to refer to the port and interface type, e.g. interface “gig-1/1/1:4”.
- Services also have Service Distribution Points (SDP)
  - SDPs are logical references to router-router tunnels.
  - SDPs are associated with LSPs.
  - VPRNs can auto-bind to SDPs based on MP-BGP information
  - L2 services require static assignment to SDP (unless VPLS BGP-AD or RADIUS config is in use).
- It’s all about abstraction!

Initial Configuration Checklist

- The following items should be configured at initial system configuration:
  - Admin password
  - Host name
  - Domain name and DNS server address
  - Configuration file location
  - System logging
  - Out of band management
  - Default and backup routers for management
  - Configure remote access services
  - User accounts
  - System time
  - System and transient interfaces
  - Remaining configuration needed to put the router into service (protocols, filters, etc)

Initial Configuration

- Log in as admin

```
Login: admin
Password: admin
*A:NS065051303#
```

- Create blank config file (save and quit vi with :wq)

```
*A:NS065051303# file vi cf3:\workshop.cfg
```

- Configure BOF parameters

```
*A:NS065051303# bof primary-config cf3:\workshop.cfg
*A:NS065051303# bof save
```

- Configure router name

```
*A:NS065051303# configure system name <<name>>
*A:<<name>>#
```

- Configure router domain name

```
*A:NS065051303# bof dns-domain <<domain-name>>
```

- Configure name server address

  - `*A:NS065051303# bof primary-dns <<dns-server>>`

Initial Configuration

- Adjust logging parameters if needed.
  - Default log 99 is configured.
  - Additional logging destinations may be configured (e.g. syslog)
- Commit changes so far
  - admin save
  - bof save

Initial Configuration

- Configure system services for remote access
  - `configure system security ssh preserve-key`
  - `configure system security ssh no server-shutdown`
  - `configure system security telnet[v6]-server`
  - `configure system security ftp-server`
- Configure banner
  - `configure system login-control banner`
  - `configure system login-control motd`
  - `configure system login-control pre-login-message`
- Configure user accounts
  - Define roles
    - Super-user
    - Read Only
    - Read Write
  - `configure system security profile`
  - `configure system security user`

Initial Configuration

- Configure time zone and manually set the time of day
  - `configure system time zone`
  - `admin set-time`
- Configure NTP
  - `configure system time [s]ntp <<server>>`
- Configure cards
  - `configure card 1 card-type iom-9g`
  - `configure card 1 card-type iom3-xp`
- Configure MDAs
  - `configure card 1 mda 1 mda-type m1-1gb-sfp`
  - `configure card 1 mda 1 mda-type m10-1gb-xp-sfp`
- Configure system interface
  - `configure router interface “system” address` <u>`x.x.x.x/32`</u>
  - `configure router interface “system” address` <u>`X:X:X:X/128`</u>
  - `configure router interface “system” no shutdown`

Initial Configuration

- Configure port 1/1/1
  - `configure port 1/1/1` **`network`**
  - `configure port 1/1/1 ethernet ?`
- Configure interface to Internet network
  - `configure router interface “to-internet”`
  - `address X.X.X.X/24`
- Use descriptions
- Consider other options you might want:
  - MTU
  - Encapsulation (dot1q, qinq, null…)
  - Speed/duplex

- configure router (bgp|ospf|mpls|ldp|…)

CLI Comparison

JUNOS	IOS	SR-OS
set date	clock set	admin set-time
ping	ping	ping
request system reboot	reload	admin reboot
request message	send	write
show system uptime	show version	show uptime
show chassis environment	show environment	show chassis environment
show cli history	show history	history
show log [file <name>]	show log	show log log-id <nn>
show system processes	show process	show system cpu
show configuration	show running-config	admin display-config
request support information	show tech-support	admin tech-support
show system users	show users	show users
show version show chassis hardware	show version	show version show card show mda
set cli screen-length	terminal length	environment terminal length
set cli screen-width	terminal width	Should auto size
trace	traceroute	traceroute

www.alcatel-lucent.com

Afternoon workshop

ALU: admin/admin

JNPR: lab/lab123

Cisco: none

1. Login to each box
2. Review configuration
    1. admin display-config
    2. show running-config
    3. show configuration
3. Create username and passwords
4. Configure the Internet-facing ports with IP addresses per lab diagram
5. Ensure end-to-end connectivity (ping)

http://192.168.175.70/security-workshop/