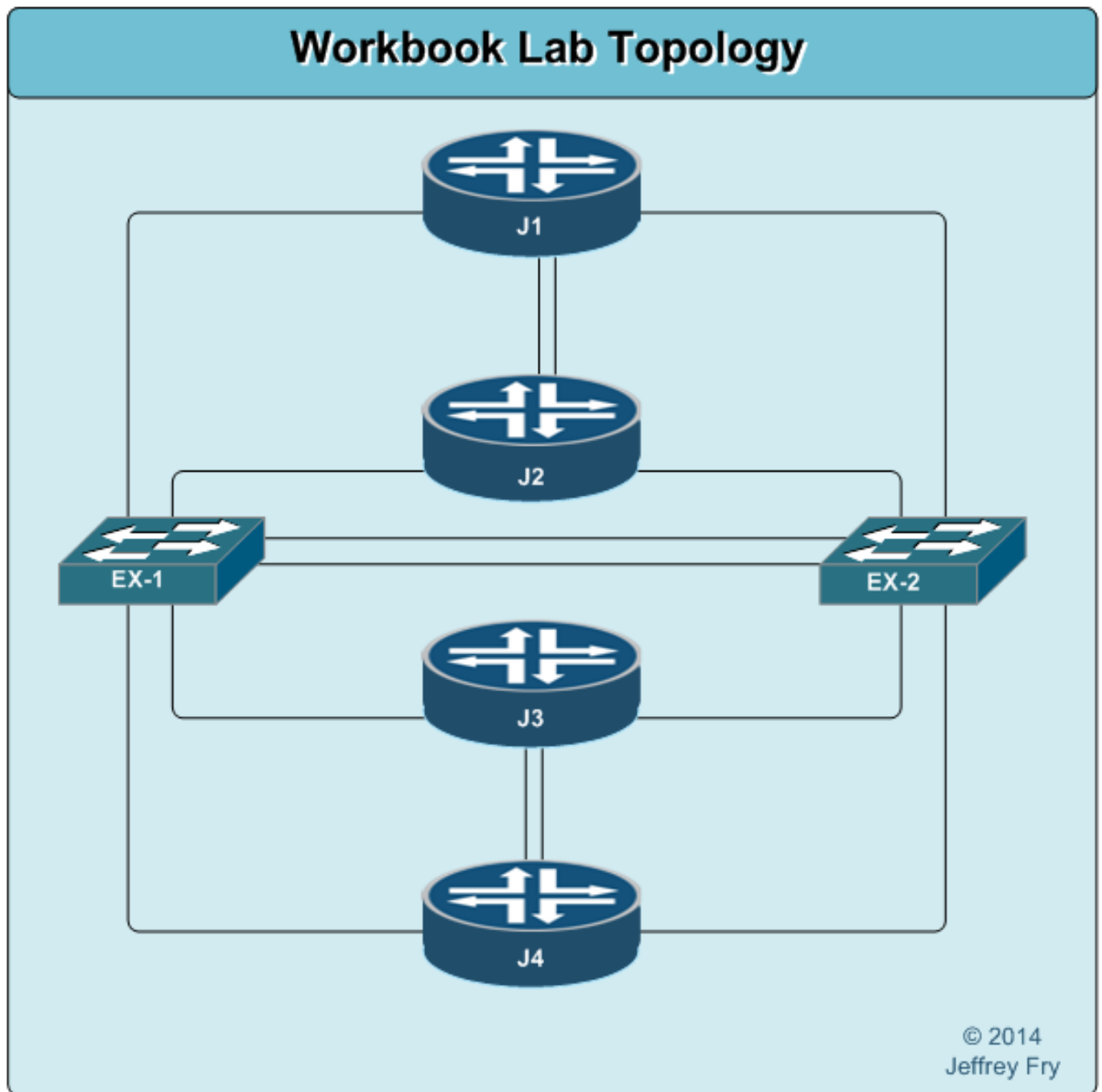


# The *Unofficial* JNCIE-ENT

## Prep Guide



# The Unofficial JNCIE-ENT Prep Guide

A guide to help you prepare for your JNCIE-ENT Lab exam

Jeffrey Fry

This book is for sale at <http://leanpub.com/JNCIE-ENT>

This version was published on 2015-09-17



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

©2014 - 2015 Jeffrey Fry

## **Tweet This Book!**

Please help Jeffrey Fry by spreading the word about this book on [Twitter](#)!

The suggested hashtag for this book is [#JNCIEPrep](#).

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

<https://twitter.com/search?q=#JNCIEPrep>

# Contents

Preview . . . . .	1
<b>About this guide . . . . .</b>	<b>5</b>
Recognition . . . . .	5
Errata . . . . .	6
Future . . . . .	6
<b>Updates and Changes . . . . .</b>	<b>7</b>
<b>Juniper Certification Overview . . . . .</b>	<b>9</b>
<b>Lab Location (US), Scheduling, and Information . . . . .</b>	<b>10</b>
<b>Lab setup for this guide . . . . .</b>	<b>11</b>
<b>System Services and Security (Preview) . . . . .</b>	<b>13</b>
System Services . . . . .	13
NTP . . . . .	13
<b>Ethernet Switching (Preview) . . . . .</b>	<b>19</b>
Spanning Tree Protocol . . . . .	19
STP . . . . .	19
VSTP . . . . .	22

## Preview

This is just a sample of two of the chapters in this workbook, System Services and Ethernet Switching.

As of this preview publishing, the current table of contents is below (this is subject to change as I finish the workbook):

### Contents

About this guide

Updates and Changes

Juniper Certification Overview

Lab location and scheduling

Lab setup for this guide

System Services and Security

- System Services
- NTP
- Syslog
- Authentication and Authorization
- Configuring Archival
- RPM
- Securing the Control Plane
- Stateless firewall configuration

### Interfaces

- Implementation
- Aggregated Ethernet
- VRRP
- Ethernet OAM
- GRE Tunnels
- BFD
- Logical Tunnel Interfaces

### Ethernet Switching

- Spanning Tree Protocol
- STP
- VSTP
- RSTP
- MSTP and CIST

- xSTP interoperability and Multiple Topologies
- Optimization
- VLANs
- VLAN switching and trunking
- Q-in-Q
- LAYER 2 Protocol Tunneling
- IP Telephony
- Private VLANs
- Virtual Chassis
- Master determination
- Add/remove members
- VCP and VCEP interfaces
- Split detection
- Breaking up a Virtual Cluster
- Security Features
- Port security features
- Dynamic ARP inspection and DHCP snooping
- Layer 2 firewall filters and other features
- MAC table filtering
- Other Layer 2 Security

## IGPs

- OSPF
- DR/BDR Routers
- Single Area OSPF
- Network and link types
- Adjacency Optimization
- Multi-area OSPF topologies
- Filter and summarize routes
- OSPF LSA
- Other OSPF
- Metrics
- Reference Bandwidth
- Dynamically Adjusting OSPF Interface Metrics Based On Bandwidth
- OSPF Preference Values
- OSPF BFD
- RIPv2
- OSPFv3
- RIPng
- Redistribution

**BGP**

- Implementation and Troubleshooting
- EBGp
- Route selection
- BFD
- More BGP / Routing policy
- **Protocol Independent Routing**
- Load Balancing
- Filter-Based Forwarding
- Configuring Routes

**Multicast**

- Implementation of Multicast
- PIM Dense Mode
- PIM Sparse Mode
- Anycast RP
- Anycast RP with MSDP
- Source Specific Multicast SSM
- Multicast Listener Discovery MLD
- Interdomain MSDP
- EX and IGMP

**Class of Service**

- Loss priority
- Packet Classification
- Multifield Classifiers and Behavior Aggregate Classification
- Rewrite rules
- Drop Profiles
- Shaping and policing
- Scheduling
- Putting it all together - Scheduling Configuration

**Appendix A -Important Notes**

- Common Ports
- Default Route Tables
- Regular Expressions
- Firewall Filters Review

- Rename, Copy, Replace
- How to specifically filter output in a command
- Commit, Commit Confirmed
- Logical Tunnels and IPv6 in Junos
- Routing Protocol Preferences Values

## **Appendix B - IPv6 Primer**

- IPv6 Refresher

## **Appendix C - Multicast Information**

- VLC Multicast Server Setup
- Windows Server 2003 IPv6
- Ubuntu Client Screen Shot



# About this guide

I am writing this guide as I prepare for my JNCIE-ENT lab exam that is scheduled in late 2014. I figured the best way for me to be sure I learn the subject is to write what I have learned and share that with the reader. I think it is called *learning by Teaching*<sup>1</sup>.

It is not my intention of this guide to be in any competition with other workbook vendors. My goal is more of a preparation guide to help others get ready prior to using those workbooks. This is also my way of working through the JNCIE-ENT syllabus that Juniper has posted so that I know I hit all the topics as well as learn as much as I can about them.

Over the past few years of blogging at [www.fryguy.net](http://www.fryguy.net) I have “[published](#)<sup>2</sup>” workbooks on [NX-OS](#)<sup>3</sup> for the Nexus 7000, [IOS-XR](#)<sup>4</sup> for the ASR9K, and most recently a workbook on [Learning Junos](#)<sup>5</sup>. Now is the time for me to step it up with a good Preparation workbook – something with a goal that equates to more than just learning a topic. It’s time to help others become an expert.

As I write this guide in [Markdown](#)<sup>6</sup>, I am assuming that you are already familiar with Junos and have achieved the JNCIS-ENT and JNCIP-ENT certifications. I will cover topics in as much detail as possible. I am using the [currently published syllabus JPR-943](#)<sup>7</sup> as of 9/14 as my guide to writing this. So some things might seem a bit out of order (like configuring services before configuring interfaces).

A little housekeeping on the format.

Configurations are in the following format:

[edit]

```
jfry@J1# set interfaces lo0 unit 0 family inet address 1.1.1.1/32
```

[edit]

```
jfry@J4# set interfaces lo0 unit 0 family inet address 4.4.4.4/32
```

## Recognition

I also want to take a moment and thank [Tim Hoffman](#)<sup>8</sup>, [Steve Rossen](#)<sup>9</sup>, and [Greg Ferro](#)<sup>10</sup> for helping me with this book as well as motivating me to write this guide. Steve and Tim have been great technical resources

---

<sup>1</sup>[http://en.wikipedia.org/wiki/Learning\\_by\\_teaching](http://en.wikipedia.org/wiki/Learning_by_teaching)

<sup>2</sup><http://www.fryguy.net/published-workbooks/>

<sup>3</sup><http://www.fryguy.net/published-workbooks/nexus-7000-training/>

<sup>4</sup><http://www.fryguy.net/2012/10/19/ios-xr-workbook/>

<sup>5</sup><http://www.fryguy.net/2014/01/13/junos-workbook-volume-1-full/>

<sup>6</sup><http://en.wikipedia.org/wiki/Markdown>

<sup>7</sup>[http://www.juniper.net/us/en/training/certification/resources\\_jncieent.page](http://www.juniper.net/us/en/training/certification/resources_jncieent.page)

<sup>8</sup><http://blog.hoff.geek.nz/>

<sup>9</sup><http://steverossen.com/>

<sup>10</sup><http://etherealmind.com/>

who have helped to make this guide what it is today. Greg has been a great person to [motivated](#)<sup>11</sup> me to get this workbook done.

Why [LeanPub](#)<sup>12</sup>?

Why did I chose to publish this study guide using LeanPub? At the Cisco Live 2013 conference in Orlando, FL, Greg and I had a great discussion over electronic book publishing. He showed me the book he has, *The Arse First Method of Technical Blogging*<sup>13</sup>, that was writting using LeanPub. He informed me that you have full control over just about all the aspects of the book and publishing. Things from the selling prices to discounts, as well as - and this is what really had my attention - the ability to notify users of updates.

With the [NX-OS, IOS-XR, and Junos workbooks](#)<sup>14</sup> I have written over the years, once they are done and published on the blog, I do not have a way to notify people who have them about updates or changes. Using LeanPub I will be able to overcome that issue and notify the readers when an update is made. As with any study guide, there will be changes over time as technologies and tests change as well as errors are noticed and corrected..

## Errata

I will be the first to admit it, I am human and I make mistakes. While I have done all that I can to make this book error-free, I know that it is not. If you notice an error in this book, please let me know at [jeff@fryguy.net](mailto:jeff@fryguy.net)<sup>15</sup> and I will check and make any necessary changes. The more information that you can provide me, the better we can make this guide.

## Future

Is is my intention to make updates, changes, and additions to this guide as time goes on. As new things are rumored to be added to the test, I will try and add them to this guide. If I learn or see something useful to the test, I will add it. If you think that something needs to be added, please let me know at [jeff@fryguy.net](mailto:jeff@fryguy.net)<sup>16</sup> so that I may add it to the guide.

---

<sup>11</sup><http://etherealmind.com/response-published-workbooks-at-fryguys-blog/>

<sup>12</sup><https://leanpub.com/JNCIE-ENT>

<sup>13</sup><https://leanpub.com/Technical-Blogging-Writing-Arse-First>

<sup>14</sup><http://www.fryguy.net/published-workbooks/>

<sup>15</sup><mailto:jeff@fryguy.net>

<sup>16</sup><mailto:jeff@fryguy.net>

# Updates and Changes

Over time I anticipate making updates and changes to this guide. The test will change over time, topics will be added and removed, and new technology may be introduced that should be included. When I make those changes, I will post notes on the changes in this section.

## January 2014

- Initial creation of the guide.

## May 2014

- Half way done mark!

## October 2014

- Rough draft completed and in editing mode.

## October 31, 2014

- Initial Publishing

## March/April 2015

- Removed console password showing in one of the configs.
- Fixed some spelling issues. (Thank you, David Y )
- Reworded and clarified some NTP settings.
- Fixed some command errors in the *firewall* stanza.
- Added testing environment information (Keyboard/Mouse/Monitor)

## June/July 2015

- Fixed some stanza errors in multiple sections.
- Updated Virtual Chassis Section
- Updated OSPF section and fixed some errors (missing commands)
- Fixed OSPF3 IPv4 routing table as screen grab was too soon.
- Fixed some table formatting
- Updated lab documentation information based on [J-Net Forum post](http://forums.juniper.net/t5/Training-Certification-and/Documentation-available-during-JNCIE-ENT-lab/td-p/139347)<sup>17</sup>.

---

<sup>17</sup><http://forums.juniper.net/t5/Training-Certification-and/Documentation-available-during-JNCIE-ENT-lab/td-p/139347>

- Updated route redistribution section to include tags as well as some additional information for OSPF<->OSPF3
- Added information on BGP for IPv6
- Added BGP as-path filtering
- Cleaned up BGP routing tables misalignments

### **August 2015**

- Added IPv6 over IPv4 BGP peering

### **SEPTEMBER NOTE**

I am actively working on updates now and will be publishing some more updates soon. If there is something you would like to see, please let me know at [jeff@fryguy.net](mailto:jeff@fryguy.net)

# Juniper Certification Overview

Juniper certifications are available from Associate, Specialist, Professional, to Expert. There are three primary tracks for Juniper Certifications: Enterprise, Service Provider and Security. There are also a few other technology tracks, like Q-Fabric for example.

	Enterprise	Service Provider	Security
Expert	JNCIE-ENT JPR-943 Hands-on LAB	JNCIE-SP JPR-960 Hands-on LAB	JNCIE-SEC JPR-932 Hands-on LAB
Support Professional	JNCSP-ENT JN0-694 (optional)	JNSP-SP JN0-692 (optional)	JNCSP-SEC JN0-696 (optional)
Troubleshooting	Junos Troubleshooting – JN0-690 (optional)		
Professional	JNCIP-ENT JN0-643	JNCIP-SP JN0-660	JNCIP-SEC JN0-633
Specialist	JNCIS-ENT JN0-343	JNCIS-SP JN0-360	JNCIS-SEC JN0-332
Associate	JNCIA-JUNOS JN0-102		

The Associate, Specialist, and Professional level tests are all computer based exams taking at a local testing center that has been authorized by Juniper to give the tests. The Support level exams are optional and not required for the JNCIE, but they are key to helping you develop your troubleshooting skills. The Expert level tests are 8-hour, hands-on lab exams that are given by Juniper at Juniper facilities.

The focus of this guide will be on the expert level certification test for Enterprise, the JNCIE-ENT.

You can find more information about Juniper certifications on the Juniper.net website at [Juniper.Net](http://www.juniper.net/us/en/training/certification/certification-tracks/)<sup>18</sup> certification site. The chapters for this book are taken from the JNCIE-ENT Exam Objectives as of January 2014. You can see the current objectives at this [LINK](http://www.juniper.net/us/en/training/certification/resources_jncieent.html)<sup>19</sup>.

---

<sup>18</sup><http://www.juniper.net/us/en/training/certification/certification-tracks/>

<sup>19</sup>[http://www.juniper.net/us/en/training/certification/resources\\_jncieent.html](http://www.juniper.net/us/en/training/certification/resources_jncieent.html)

# Lab Location (US), Scheduling, and Information

To schedule the JNCIE-ENT lab you will need to log into the Juniper Exam Registration website at <https://juniper.my-certifications.com/Sites/Candidate/Default.aspx><sup>20</sup>. Once you have logged in, you select Schedule a JNCP Lab Exam – that is the JNCIE lab exam – and then read and accept the agreements for the test.

You first select your region ( Americas, APAC, or EMEA) and then your country, and then the lab exam you want to take. Lastly, you select a range of dates that you would like to take the test and the system will return the available dates that you can select from.

For the Americas, the JNCIE-ENT lab is only available at two locations – Herndon, VA and Sunnyvale, CA. Also, unlike another vendor's expert level test, tests are not given every day but only a few times a month. So be aware that the testing availability dates are limited right now.

When you go to take your lab exam, try to get in early the day before so that you can familiarize yourself with the location of the lab, how to get there, where to park, doors, etc. The more information you have the day before the more comfortable you will be the day of. It is also been mentioned that you may want to bring your own keyboard, mouse, and maybe even monitor to the test with you. The lab is given on a laptop at the Juniper location, so the keyboard and screen are relatively small. I would suggest touching base with Juniper prior to your lab, but this is something to consider.

You will also have access to some Juniper documentation in the form of PDFs located on the desktop of your workstation. You can find the information contained in them at these two links: [Junos OS Documentation](#)<sup>21</sup> [Junos OS Documentation for EX Series](#)<sup>22</sup>

Make sure you get a good nights sleep, eat a good breakfast, and dress comfortably. You will not be graded on your attire, but I would urge you to dress respectable. I would also arrive at the test center at least 30 minutes early to make sure you are there - never know what traffic you may encounter. The lab duration is 8 hours, not including your lunch hour - so plan to be at the facility for 9 hours.

After you are done with your test you should be prepared to wait for your results as they may take up to 15 days to receive.

---

<sup>20</sup><https://juniper.my-certifications.com/Sites/Candidate/Default.aspx>

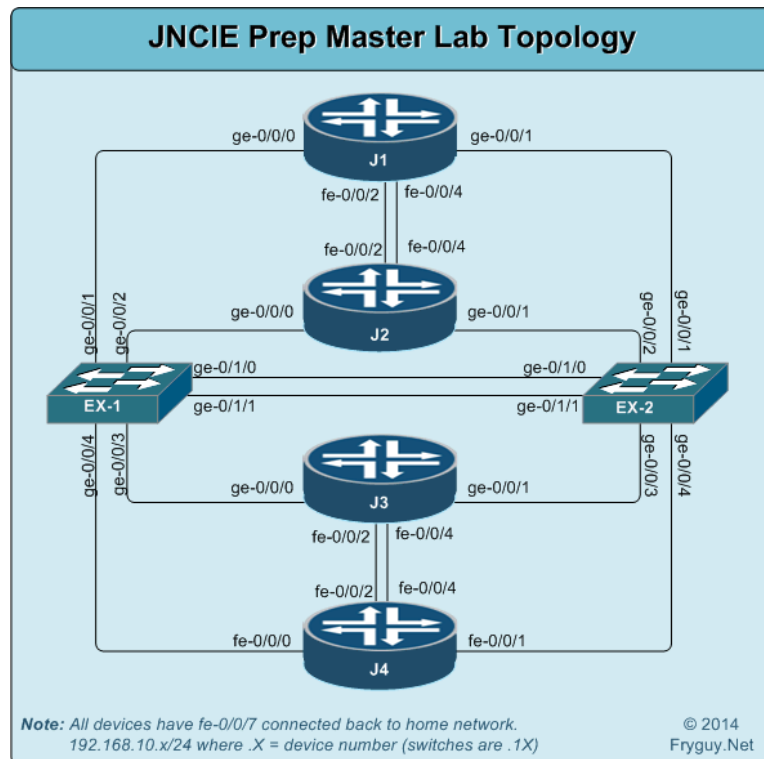
<sup>21</sup>[http://www.juniper.net/techpubs/en\\_US/junos10.4/information-products/pathway-pages/product/10.4/index.html](http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/product/10.4/index.html)

<sup>22</sup>[http://www.juniper.net/techpubs/en\\_US/junos10.4/information-products/pathway-pages/ex-series/index.html](http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/ex-series/index.html)

# Lab setup for this guide

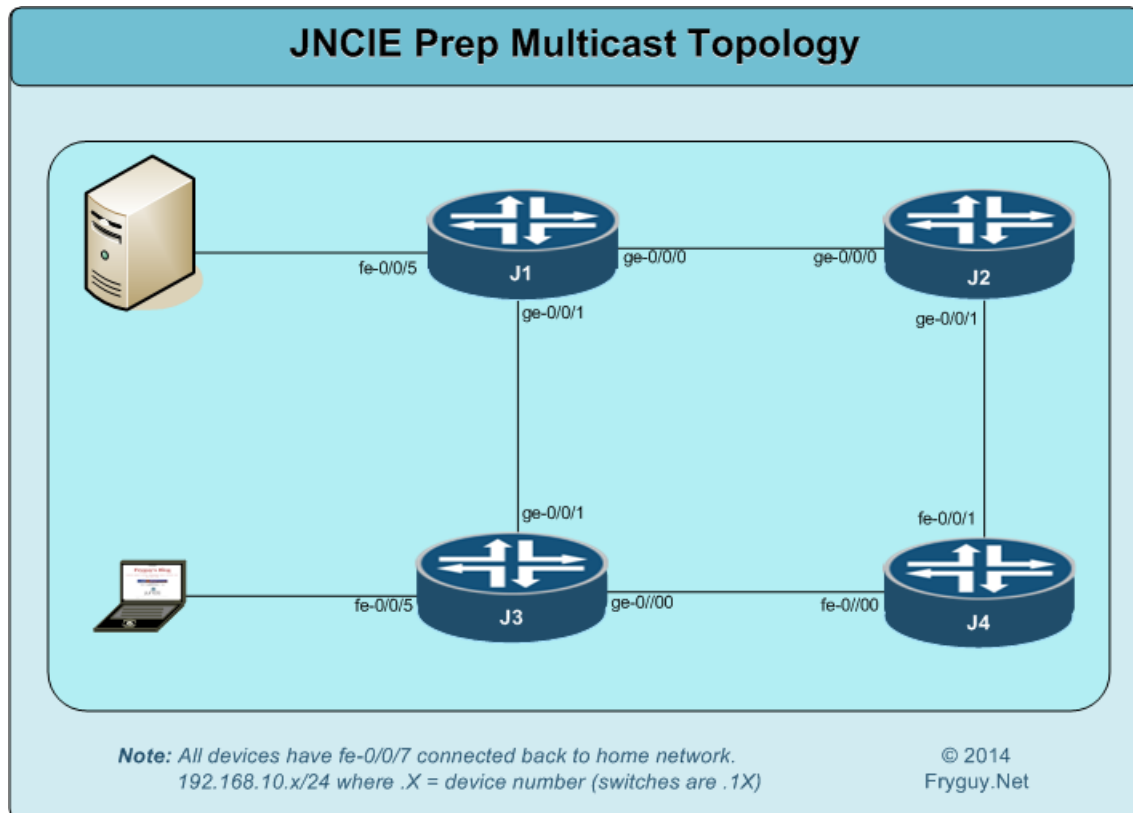
Below is the topology that has been used throughout this workbook. It consists of three (3) Juniper SRX210H routers, one (1) Juniper SRX100H router, and two (2) Juniper EX-2200C switches. The Junos code on the SRX routers is 12.1R2.9 and the EX2200 switches are running 12.3R3.4 code.

Below is a lab topology diagram that we will use throughout this workbook.



When it comes to IP addresses, we will use a standard workbook type scheme - 10.1.X.Y where X is Router to Router Number (ie J1 to J2 would be 12) and Y is the router number (ie J1 is .1). The switches will be .11 for SW1 and .12 for SW2. Loopbacks will be X.X.X.X/32 on all devices.

Later on in this guide we will be discussing and demonstrating multicast. When it comes to the multicast section we need to note that we have an Ubuntu machine connected to J1 on interface fe-0/0/5 and a Windows machine connected to J3 on interface fe-0/0/5.



Please note that on each devices, fe-0/0/7 is may be using 192.168.10.x/24 with a gateway of 192.168.10.254. This interface is connected to a Layer 3 switch that will allow connections back to my home network. On my home network I have a server at 192.168.0.3 running for connections from the lab. This connection will be used for system services connection (ntp, auth, syslog, etc) and Jweb access from outside the lab network.



# System Services and Security (Preview)

---

## System Services

The first topic on the JNCIE-ENT syllabus in System Services. These services are found under *edit system-services* in the configuration. Their purpose is to help the Junos device communicate on the IP network for the requested services.

---

## NTP

Network Time Protocol, or NTP, is defined under [RFC5905](https://tools.ietf.org/html/rfc5905)<sup>23</sup>, uses UDP port 123, and used for synchronizing the system clock to an NTP server. Each NTP server is defined by a stratum number, with 1 being a Primary server, and every server below that is defined by one greater. The maximum strata level is 16 and called MAXSTRAT.

Junos devices can be configured to act as a NTP Client, NTP Secondary Server, or NTP Primary Server. The Primary NTP server is synchronized to a reference clock and then makes this information available to downstream NTP servers and clients. A Secondary NTP server are synchronized to the Primary NTP server, and like the primary, make this information available to downstream clients and servers. Finally, a NTP client is synchronized to a NTP server and do not distribute this information to any other devices.

Each client is capable of being configured to run in one or more of the following modes:

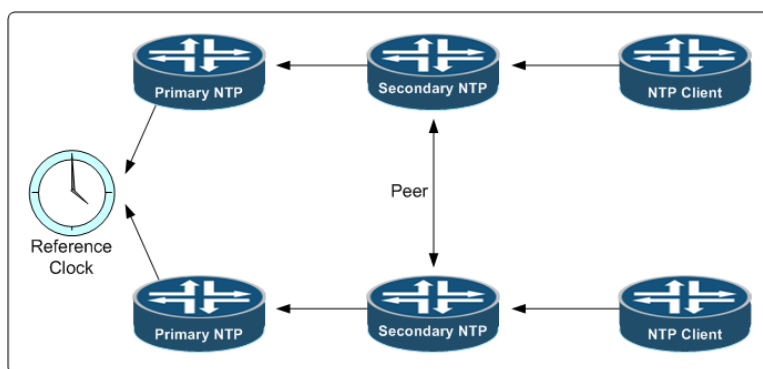
**Broadcast Mode** - Transmits the time information via broadcast or multicast addresses. Devices on the network listen for this and sync their clocks based on this information. This mode is the least accurate of the modes.

**Client/Server Mode** - Devices are configured in an hierarchical format with a Server providing the NTP server providing time to the NTP Clients. The NTP clients pull this information from the server.

**Symmetric Active Mode (Peer)** - In peer mode, two devices peer and sync their time information between each other.

---

<sup>23</sup><https://tools.ietf.org/html/rfc5905>



NTP Stratum Representation

The diagram above depicts a reference clock on the left and routers that have been identified as Primary, Secondary, and Client devices.

For the lab, I have a NTP server configured at IP address 192.168.0.6.

The pertinent existing configuration on J1 is:

```
jfry@J1> show configuration system ntp
```

```
jfry@J1> show system uptime
```

```
Current time: 2014-01-01 10:41:42 UTC
```

```
System booted: 2014-01-01 02:52:48 UTC (07:48:54 ago)
```

```
Protocols started: 2014-01-01 02:55:45 UTC (07:45:57 ago)
```

```
Last configured: 2014-01-01 10:40:42 UTC (00:01:00 ago) by jfry
```

```
10:41AM up 7:49, 1 user, load averages: 0.33, 0.18, 0.06
```

```
jfry@J1>
```

```
jfry@J1> show configuration interfaces fe-0/0/7
```

```
unit 0 {
```

```
family inet {
```

```
address 192.168.10.1/24;
```

```
}
```

```
}
```

```
jfry@J1>
```

As you can see, the current system clock is set to UTC as well as shows the date and time as January 1st, 2014 at 10:41 AM. The current date and time is actually February 3, 2014 21:26PM UTC. Since we are so far out of sync (more than 128 seconds), we actually need to bring the clocks closer together manually first or set a max-adjustment setting. Since setting the system clock manually is easier, we will do that.

To set the time manually we use the command *set date YYYYMMDDhhmm.ss*, as you can see in the command output below, in CLI mode.

```
jfry@J1> set date ?
Possible completions:
  <time>          New date and time (YYYYMMDDhhmm.ss)
  ntp             Set system date and time using Network Time Protocol servers
```

So let's set the date to Feb 3, 2013 at 21:30 UTC

```
jfry@J1> set date 201402032130.00
Mon Feb  3 21:30:00 UTC 2014
```

```
jfry@J1>
```

There, now we can configure NTP on the router. To configure NTP, you will need to navigate to the *edit system ntp*..

```
[edit]
jfry@J1# edit system ntp
```

Once there we have a few *set* options available to us:

```
[edit system ntp]
jfry@J1# set ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> authentication-key   Authentication key information
  boot-server          Server to query during boot sequence
> broadcast             Broadcast parameters
  broadcast-client     Listen to broadcast NTP
> multicast-client      Listen to multicast NTP
> peer                 Peer parameters
> server               Server parameters
  source-address       Use specified address as source address
+ trusted-key           List of trusted authentication keys

[edit system ntp]
jfry@J1# set
```

First up we will look at the *boot-server* command. The *boot-server* command is used by the router when it first boots up. It will query, on initial load, the configured boot server to set the system clock. After that, the configured NTP server will take over to maintain the system clock.

To set the boot server to 192.168.0.6, use the following command:

```
[edit system ntp]
jfry@J1# set boot-server 192.168.0.6
```

If we want the router to be a broadcast/multicast server, we use the command *set broadcast* command.

```
jfry@J1# set broadcast ?
Possible completions:
<address>          Broadcast or multicast address to use
```

Here you can see you can either set the broadcast or multicast address. You can also set the ttl, version, and authentication if necessary.

To set the broadcast or multicast client, you can use the *set broadcast-client* or *set multicast-client (address)* command.

```
[edit system ntp]
jfry@J1# set broadcast-client
```

```
[edit system ntp]
jfry@J1# set multicast-client ?
Possible completions:
<[Enter]>          Execute this command
<address>          Multicast address to listen to
|                  Pipe through a command
```

To set a NTP peer, you use the command *set peer (address)* command.

```
[edit system ntp]
jfry@J1# set peer ?
Possible completions:
<address>          Name or address of peer
```

Finally, to set the NTP server, use the *ntp server (address)* command.

```
[edit system ntp]
jfry@J1# set server 192.168.0.6 ?
Possible completions:
<[Enter]>          Execute this command
key                Authentication key
prefer             Prefer this peer_serv
version            NTP version to use (1..4)
|                  Pipe through a command
```

```
[edit system ntp]
jfry@J1# set server 192.168.0.6
```

If necessary, like it is in this lab, you can set the source-address using the *set source-address* command.

```
[edit system ntp]
jfry@J1# set source-address 192.168.10.1
```

```
[edit system ntp]
jfry@J1#
```

Here is the config we will use to set the NTP server on this client:

```
[edit system ntp]
jfry@J1# show
boot-server 192.168.0.6;
server 192.168.0.6;
source-address 192.168.10.1;

[edit system ntp]
jfry@J1#
```

Now we can commit it and check the system clock *Note - I stepped away while writing this and the current time is now 2:13 AM UTC on February 4, 2014.*

```
[edit system ntp]
jfry@J1# commit and-quit
```

To check to see if you are synced to the NTP server, you use the command `show ntp associations`.

```
jfry@J1> show ntp associations
remote      refid st t when    poll reach  delay  offset  jitter
=====
192.168.0.6 .INIT. 16 -   -      64     0   0.000   0.000  4000.00
```

While in the .INIT. state, you are not synced and may be in the process. After a few moments, run the command again.

```
jfry@J1> show ntp associations
remote      refid st t when    poll reach  delay  offset  jitter
=====
192.168.0.6 .STEP. 16 - 1594    64     0   0.000   0.000  4000.00

jfry@J1>
```

Here you can see that we are now synced with a Stratum 16, we poll ever 64 seconds, and we have no delay/offset as we are “local” to the server. If a server is further away, you will see different values here.

Now we can look at the `show system uptime` command again and check the time:

```
jfry@J1> show system uptime
Current time: 2014-02-04 02:21:04 UTC
System booted: 2014-02-03 14:36:47 UTC (11:44:17 ago)
Protocols started: 2014-02-03 14:39:43 UTC (11:41:21 ago)
Last configured: 2014-02-04 01:15:12 UTC (01:05:52 ago) by jfry
  2:21AM up 11:44, 1 user, load averages: 0.09, 0.18, 0.08

jfry@J1>
```

What if we want to have some security around our NTP servers? To do that we will need to create some trusted-keys on our NTP server and our clients.

```
[edit]
jfry@J1# set system ntp authentication-key 1 type md5 value password

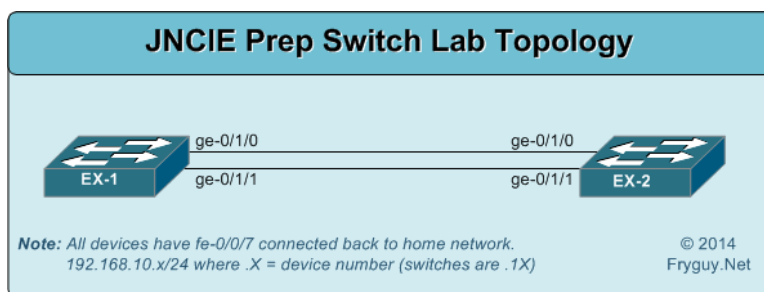
[edit]
jfry@J1# set system ntp trusted-key [1]

[edit]
jfry@J1# set system ntp server 192.168.0.6 key 1
```

Once that is committed, we will only synchronize with a server that is also using that key.

# Ethernet Switching (Preview)

Ethernet switching is a very large topic to cover. We cover from RSTP, VSTP, MSTP, VLANs, QinQ, PVLAN, Virtual Chassis, Port Security, and beyond. For these labs I am using a pair of EX2200-C<sup>24</sup> switches. The EX2200-C switch is a fan-less 12-port 10/100/1000 Base-T switch with 2 100/1000Base-X ports. It supports almost everything that its larger brothers do, including Virtual Chassis, so they are really good for home labs. The few things that it does not support are BGP and Virtual-Chassis using the VC cables. I have these switches connected to each other via two 1G OM3 fiber connections on ge-0/1/0 and ge-0/1/1 as can be seen in the diagram below.



## Spanning Tree Protocol

Our first topic for switching is Spanning Tree Protocol (STP). The purpose of STP is to ensure a loop-free topology on a bridged (layer 2) Ethernet network. The purpose of Spanning-Tree is to create a single active path to the Root bridge, and any link that is not along that path is in a blocked state.

Under spanning tree, we will cover:

- STP - 802.1D
- RSTP - 802.1w
- MST - 802.1s
- VSTP - Juniper proprietary

## STP

STP is defined under 802.1D<sup>25</sup> is configured under *edit protocols stp* in the configuration stanza and builds one topology for all VLANs and forwarding. BPDUs are passed untagged on all interfaces. It is also worth noting that once you enable STP, it will be enabled for ALL interfaces. If you want to disable it for an interface, you will need to explicitly disable it on that interface.

<sup>24</sup><http://www.juniper.net/us/en/products-services/switching/ex-series/ex2200/>

<sup>25</sup><http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>

```
{master:0}[edit]
jfry@EX1# edit protocols stp

{master:0}[edit protocols stp]
jfry@EX1#
```

From here we have a few different options to explore:

```
{master:0}[edit protocols stp]
jfry@EX1# set ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  bpd-block-on-edge    Block BPDU on all interfaces configured as edge (BPDU Protect)
  bridge-priority       Priority of the bridge (in increments of 4k - 0,4k,8k,..60k)
  disable              Disable STP
  forward-delay         Time spent in listening or learning state (4..30 seconds)
  hello-time           Time interval between configuration BPDUs (1..10 seconds)
> interface
  max-age              Maximum age of received protocol bpdu (6..40 seconds)
> traceoptions          Tracing options for debugging protocol operation
```

We can configure our bridge-priority, we can disable STP on an interface, change the forwarding delay and hello timers, as well as set the max age of received bpdus.

Since we have already entered the STP stanza, we can set our *bridge-priority*. Keep in mind that this must be in increments of 4k - so 0k, 4k, 8k, 12k, etc. Lowest priority wins with the lowest MAC as the tiebreaker if priorities are the same..

```
{master:0}[edit protocols stp]
jfry@EX1# set bridge-priority 4k
```

And we can commit that on EX1 and move onto EX2.

```
{master:0}[edit]
jfry@EX2# show | compare [edit protocols]
+   stp {
+       bridge-priority 8k;
+   }
```

By default on EX2, ge-0/1/0 will be in forwarding and ge-0/1/1 will be in blocking as can be seen once EX2 configuration has been committed.



```
{master:0}
jfry@EX2> show spanning-tree interface brief
```

Spanning tree interface parameters **for** instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/1.0	128:514	128:514	8192.88e0f368d901	20000	FWD	DESG
ge-0/1/0.0	128:561	128:561	4096.40b4f0b0c041	20000	FWD	ROOT
ge-0/1/1.0	128:562	128:562	4096.40b4f0b0c041	20000	BLK	ALT

As you can see in the output above, the port costs are all the same (20000) and ge-0/1/0 is in forwarding while ge-0/1/1 is in blocking. This was determined by the port-id as 128:561 is lower than 128:562. In the event of a tie in cost, port-id will win.

So let's change the cost on ge-0/1/1 to a cost of 1 (lower number wins)

```
{master:0}[edit]
jfry@EX2# set protocols stp interface ge-0/1/1 cost 1
```

And to verify we can look at our *show spanning-tree interface brief* output.

```
{master:0}
jfry@EX2> show spanning-tree interface brief
```

Spanning tree interface parameters **for** instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/1.0	128:514	128:514	8192.88e0f368d901	20000	FWD	DESG
ge-0/1/0.0	128:561	128:561	4096.40b4f0b0c041	20000	BLK	ALT
ge-0/1/1.0	128:562	128:562	32768.40b4f0b0c041	1	FWD	ROOT

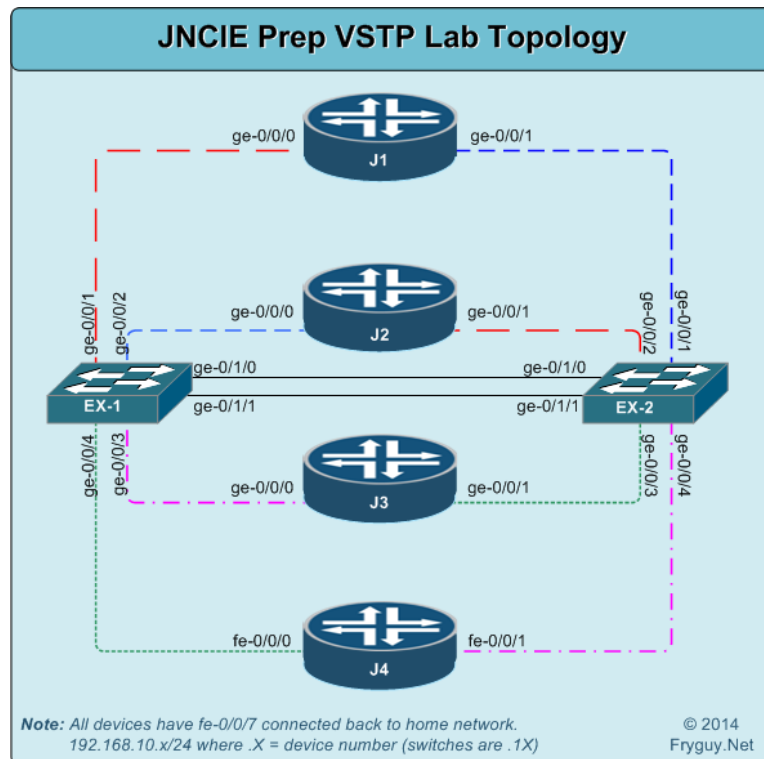
Now you will see that ge-0/0/1 is in a forwarding state as well, and if you recall STP can take up to 45 seconds to move a port to forwarding state. In order to move this port into a forwarding state quicker, you configure the port as *port-mode access* under *family ethernet-switching*

```
{master:0}
jfry@EX2> show configuration interfaces ge-0/0/1
unit 0 {
    family ethernet-switching {
        port-mode access;
    }
}
```

## VSTP

We will now turn our attention to VLAN Spanning Tree Protocol (VSTP). This flavor of spanning-tree runs a spanning-tree instance for each VLAN on the network, much like Cisco PVSTP. VSTP can inter-operate with Cisco PVST as well as Rapid-PVST switches. For more information on interoperability, you can find it on Junipers Technical Documentation page here - [VLAN Spanning Tree Protocol<sup>26</sup>](http://www.juniper.net/techpubs/en_US/junos11.4/topics/concept/mx-series-vlan-stp.html). VSTP is also the only form of STP in which BPDUs are passed as tagged frames. Additionally, it is worth noting that while VSTP, by default, maintains equivalency with Cisco PVLAN-Rapid, this can be changed to be like PVLAN-Standard.

For this lab we will be using the diagram below.



<sup>26</sup>[http://www.juniper.net/techpubs/en\\_US/junos11.4/topics/concept/mx-series-vlan-stp.html](http://www.juniper.net/techpubs/en_US/junos11.4/topics/concept/mx-series-vlan-stp.html)