

Switch setup secure and reliably

Welcome to the page where I will try to describe how to setup a managed ethernet switch in a secure and reliable way.

The purpose of this publication is show people

- how to setup and configure an ethernet switch for production environments

You might think this is not needed - just unpack, plug in and use the damn thing. WRONG!

Configuring a switch means keep control of the switch and make sure you get your moneys worth.

Prereqs

For this page it is assumed that you have bought a managed switch that you want to use in a production network, could be some enterprise network or it could be your home network. By production I think of networks that should "just work" without constant messing with it.

At my home I have several pieces of equipment being used by the rest of the family and I consider the network in production, and so does my wife - she will call me within 5 minutes if there are problems ;-)

I also consult at large companies around Denmark and I think the guide below is suitable for those environments.

I have developed this specific guide while configuring a new switch for the home network, a [Linksys SRW-2008](#) 8-port Gigabit switch with a really nice set of features, including 802.1q, SSH etc.

Initial setup

Start by unpacking the switch and check the contents of the package. Most likely you will find everything in place, but it sure would be annoying if you have misplaced the rack brackets when it is time to mount the switch. Feel free to save or throw away the box it was delivered in.

Burn in - phase

After unpacking plug the switch to some power at the nearest suitable place - only power.

If everything is alright it should boot and start showing status with some LED's. Leave the switch running for some days, to make sure it is in good working condition.

Feel free to leave it running and do something else or continue configuring it immediately.

This phase is to make sure it won't blow magic smoke right after being put into production. I would recommend at least a day and configuring it during that time is fine.

Checking firmware

Checking firmware is often not done, and why?!

Switches are complex and have lots of features, aka errors, bug and things that can go wrong.

You should always check firmware before configuring something complex like a switch, the vendor might have fixed a serious problem and you will save time later on.

My switch was delivered with software version:

```
OK
Running from RAM...
*****
*** Running SW Ver. 1.0.2 Date 12-Jun-2006 Time 18:01:35 ***
*****
```

The most recent firmware for that model according to vendor website is 1.0.3.

If you are unsure how to check the firmware level check the manual, most likely places to see firmware levels:

- during boot, connect to the console port - if switch has one
- at web administration interface - if switch has one
- using SNMP - advanced

To check the firmware level you need to connect something to the switch. Use a generic laptop or some dedicated setup equipment, but keep the switch from any existing production networks - since the default passwords hasn't been changed. I would recommend using the console and some terminal program, like minicom. If you find that the firmware is outdated you can check if the new firmware has features you like or fixes things that are important to you. I would always suggest upgrading to the most recent firmware as recommended by the vendor.

The version 1.0.3 firmware upgrade included a lot of nice features and some bugs that I couldn't easily disregard - so I decided to upgrade. Downloading the

3MB firmware across serial took some time, but since I hadn't configured any Ethernet yet it was easy to do. Beware that some switches need two updates files, my Linksys SRW-2016 switches both have boot and software files, and doing the wrong thing leads to some difficulty in upgrading.

Play with the switch

The next sections is what I consider the required and optional features that you should configure on you new switch. Most likely you will use the web administration interface, if you configure few switches and don't want to remember a lot of command line options from time to time.

While browsing around the web interface for the new switch try to get a feel for the features available and things you might want to take a look at later. Play with the switch, so you know what features are included and where they are.

Configure the switch - required settings

Switch Name, Contact, Location

Name the goodddaaamm thing! Put some effort into naming your switches, and make physical labels for the switches. My home network has switches named: switch1, switch2 and switch3 - not that advanced, but it really helps when you need somebody else to reboot a switch.

"Go to the switch labelled switch 1 and pull the power cord, then wait 10 seconds and plug it in again, thanks"

The information selected should be entered into the switch configuration. Often the switch has Name, Contact (technical contact) and Location - which corresponds to the information shown with SNMP.

Switch IP address

The switch is probably delivered with some default IP-address, similar to 192.168.1.254. You should decide what IP-address to use for that specific switch and enter it into the configuration.

Administrator passwords

Make sure you change the administrative passwords - note the plural. If you don't change passwords anybody with access to the network can change settings on the switch. They can reboot or otherwise make the switch unavailable, load

wrong firmware perhaps?
Change the password, now!

Network Time

You should always make sure the switch is running with the correct time settings, preferably using NTP, Network Time Protocol. Making sure the switch know correct time will make logs much more useful :-)

Administrative interface

Select administrative interface for configuring the switch in the future. From least desirable to recommended are:

- http, telnet - not recommended, but some switches don't have anything better, use only across short links that you control 100%
- https, ssh Secure Shell - recommended, encrypted and safe for use across insecure links

If you are left with Telnet and HTTP (without SSL) only then remember that you can use OpenSSH portforwarding to forward those insecure protocols across large networks.

Configure the switch - disable optional features

When a complex device is delivered it is often with all features enabled, for those situations where people just plug in and expect the device to work. That might be fine for a small network, or if people dont care - most people dont care ... I care. So hunt down and disable features that you don't need. What is not active won't hurt you later on, and the network won't see all this mysterious traffic from all kinds of devices.

Configure the switch - enable optional features

Below are some of the features that I like and could perhaps be ideas for you.

Configure logging

Most network equipment can be configured to log to a centralized syslog server,

check out the site <http://www.loganalysis.org/> for more ideas.

Configure SNMP

A real nice and usefull protocol is SNMP, Simple Network Management Protocol, which can give you all sorts of information about your switch. SNMP can also be configured to send alerts when something is wrong, SNMP traps they are called. Use something a bit random, for use in SNMP version 2 community, but nothing really secret - like a password. The security in protocol version 2 is quite bad, as the community name is transmitted in clear text across the network.

I mostly configure SNMP to allow me to configure MRTG to fetch statistics about usage on ports, and thus make SNMP read-only.

Advanced features VLANs

Basic portbased VLANs

Most managed switches I have seen allow some portbased virtual LANs, which mean that instead of having a 16-port switch you can decide that for instance ports 1-4 are separated from the others. This is nice and easy to set up, and allows for a very flexible setup, without the hassle of configuring real virtual LANs.

A single 16-port switch could for instance be divided like this:

- ports 1-4 are the outside, connection from internet, outside interface on firewall
- ports 5-8 are DMZ1 - a DMZ for mailservers and webservers
- ports 9-16 are the inside LAN

And portbased VLANs doesn't require anything special on the systems connected, everything looks just like having separate switches.

Advanced 802.1q VLANs

If you need something a bit more complicated some switches support [IEEE 802.1q](#) which are a protocol defined to support VLAN tagging where each packet being sent is marked as being for a specific virtual LAN. Having 802.1q support requires more from the device, and you should check that the switch has this before buying it - if you need it. While portbased VLANs can be found even in unmanaged switches the ones that support 802.1q are considerably more

expensive.

The Linksys switches I have bought are specifically selected for this 802.1q and SNMP, while staying at a reasonable price tag.

Why would you pay extra for this then? Because it allows you to define VLANs that span multiple switches. You can connect two switches and then say that switch1-port1 and switch2-ports1-5 are in a single VLANs separated from the rest of the ports on the switches - nice feature.

This feature is quite advanced but especially for things like Wireless LAN Access Points it is nice to connect the APs to the existing switches and then segregate the ports into a different VLAN for security issues. Then this VLAN is connected through the firewall somewhere else before the packets are allowed onto the normal inside LAN or the internet. Essentially this feature saves cables and switches, but can become quite complex!

Testing the switch configuration

If you configured something advanced like VLANs it would be a great thing to use a couple of systems to try out the connectivity on the switch.

Configuring multiple switches

Did you enjoy the web administration as much as I hated it?

Having to configure a single piece using a web interface is actually Okay. Since I don't go configuring switches all day I can't be bothered by remembering all the command line options for advanced stuff.

But if I am about to configure multiple switches with similar configurations I would much rather configure a single switch, pull the configuration file and then upload that into each switch, with small changes.

Luckily the Linksys switches allow just that, so also take a nice backup of the configuration for future reference.

Then it is time to setup the switch into the production network, remember to keep cables nice and tidy :-)

Recurring administration

When you have finished setting up the switch you should regularly check:

- check status
- check logging
- check for firmware updates
- environmental issues, make sure the switch is not blocked and getting too hot