Recommended Configuration of Switches in Campus Networks

Best Practice Document

Produced by UNINETT led working group
on LAN infrastructure
(No UFS105)

Authors: Børge Brunes, Vidar Faltinsen, Einar Lillebrygfjeld, Knut-Helge Vindheim
May 2010

Document No: GN3-NA3-T4-UFS105
Version / date: May 2010
Original language: Norwegian
Original title: “UFS 105: Anbefalt konfigurasjon for svitsjer i campusnett”
Original version / date: Revision 1 of 20 December 2007
Contact: campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT led working group on LAN infraatructure as part of a joint-venture project within the HE sector in Norway.

This translated version is based on the Norwegian counterpart approved by the Norwegian HE sector on 20 December 2007 after an open consultation period of four weeks.

The translation of this report has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n°238875, rel ating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

This document presents a recommendation regarding the configuration of switches in campus networks. Layer 2 and Layer 2+ functions are covered, but not Layer 3 (routing). The recommendation is generic. A number of configurations intended for supplier-specific layouts will support the recommendation.

The document does not deal with the design of campus networks, but focuses on the individual components and their configuration.

1 Introduction

This document provides specification of the Norwegian HE sector's recommended configuration of switches in campus networks. This translated version is based on the document approved by the Norwegian HE sector on 20 December 2007 after an open consultation period of four weeks.

The target group comprises IT managers and IT operations personnel in the HE sector.

A number of things must be taken into consideration when configuring switches in campus networks. Depending on its location, a switch may have various functions. Here we classify switches in three classes: core, branch and edge switches, as defined below. In each class, different switches with different port density and port composition (different speeds) are used. We do not discuss here the types of units which should be used, but provide a generic requirement list for layout and configuration.

2 Definitions

- **Layer 2**: Layer 2 of the OSI stack. Switches on Layer 2 cannot interpret IP addresses, but operate with MAC addresses.
- **Layer 2+**: Some switches have the ability to interpret the various characteristics of IP headers and higher levels. DHCP snooping is an example of such functionality, which is designated Layer 2+.
- **Layer 3**: This is the network layer which is capable of interpreting IP addresses. Some switches can perform routing. This document does not deal with such functions.
- **Edge switch**: A switch located in the periphery of the network, closest to the users.
- **Branch switch**: A switch which handles aggregate traffic from a number of edge switches and connects it to core switches.
- **Core switch**: A switch which is located in the core of the network and to which users are generally not directly connected; primarily a high-capacity connection to other switches and servers.
- **Client port**: A port on a switch which is connected to client machines in the network. This also includes servers, printers and other terminal equipment. Such ports have a number of properties which differ from those of network ports, in other words ports which are connected to other network components (routers, switches or base stations).

3 Physical Requirements

3.1 Assembly

Switches shall be assembled on racks and marked with easily legible names. Patching shall be achieved in a tidy manner, with emphasis on facilitating the replacement of switches if they fail. Light-emitting diodes shall be clearly visible.

3.2 Power supply

While there are no requirements for the provision of UPS or duplicated power supply to edge switches and branch switches, both are recommended for core switches. Typically, the primary power supply should be via a UPS, while the secondary supply should be from the public supply grid.

3.3 Flash

Core switches should have flash settings enabling the storage of at least two software versions. This makes it possible to configure the switch so as to revert to the previous version if new software fails at start-up.

4 Software

Software shall at all times be updated to the currently recommended version. UNINETT maintains an up to date list which should be followed.

Software should be downloaded from a local TFTP, FTP or SCP server.

5 Naming

Every switch shall be given a unique name, using a carefully considered naming convention. It is an advantage if the names provide information regarding the location and application of the switches. The name should be configured into a switch as its sysname. It should also be recorded in the DNS. The switch should also be physically labelled with the same name.

Switch ports should be named in the same way, also using a carefully considered convention. It may be natural to assign names using the jack or room number to which a port is patched, or if necessary the server name or name of another switch or router, if this is what the port applies to.

One may consider omitting port naming in connection with end users if some other method of documentation is used, for example using a management application.

6 Switch Administration

It must be possible to configure switches by means of remote login and to monitor them using SNMP. One should also consider using SNMP for configuration, at least for certain properties. While a web interface to a switch may be considered, experience shows that such an interface is in most cases unsuitable.

Only the access essential to operation should be open, and any other access should be blocked, cf. Section 6.6.

6.1 Management address

The management IP address of a switch should be located in a dedicated network for switches and network electronics. This network should also be well protected by means of an access list which permits access to operations personnel only.

6.2 Remote login (with banner)

Remote login should be performed using SSH. If Telnet is used, this should be via a secure transport route, cf. Section 6.1.

A banner should be created indicating that unauthorised personnel do not have access.

6.3 Authentication in connection with remote login

Login to a switch should be user-based. This has several advantages, among others that it is easy to deny access to personnel who are no longer employed. Personal passwords are also preferable to shared passwords. Last, but not least, the configuration archive clearly indicates who has performed which changes. User-based login should be based on RADIUS, TACACS+ or similar protocols. This facilitates the provision of different authorisations to different users.

This configuration mode often calls for an additional login following user-based login. Here the password is a shared secret, but one must be an authorised user to be able to use it. In any eventuality, routines must be in place for changing a password at pre-defined intervals.

It is extremely important that the supplier’s standard password is not used once a switch is accessible via the network. The password must be changed in connection with the initial configuration.

6.4 Saving a configuration

The newest version of a configuration should at all times be saved in the NVRAM of a switch. It shall also at all times be saved in a TFTP server, which should support version control (RCS or similar), so that a historical archive is maintained of all changes made.

6.5 SNMP access

SNMPv2c is the most commonly used protocol, and must be supported. Since this has a low level of security, system security must be based on filters which govern who is to be granted SNMP access to the unit. This can often be configured directly in a switch, which is recommended. Alternatively, access may be governed using a Layer 3 filter in the management network (cf. Section 6.1).

SNMP read must be supported. SNMP write may be considered, as it may, for example be practical for allowing shut down of the port via a management application, automated upgrades or other automated configuration. One should be aware of the risks involved in permitting SNMP write. Good protection of SNMP access is therefore very important.

6.6 Neighbour Discovery Protocol – LLDP, CDP etc.

For some time, Cisco has provided a proprietary solution for neighbour discovery, the Cisco Discovery Protocol (CDP). A standard now exists for this: IEEE 802.1AB or LLDP (Link Layer Discovery Protocol). For administrative purposes, this function should be activated. It provides considerable advantages during day-to-day operations and can also provide information which improves the management system's ability to discover topology. While it can be argued that in this way end users will receive unnecessary information, if a switch is otherwise well protected, this is considered acceptable.

If a switch supports LLDP, this should be used: alternatively a proprietary solution such as CDP should be used.

6.7 Syslogging

A switch should log error messages in its own buffer and also in an external syslog server.

Syslogging must be set to use a real-time clock, not a clock which refers to the elapsed time since the switch was last re-started.

6.8 NTP

A switch should be configured as an NTP client and will thus have a reliable clock. This is particularly important for precise logging. It can be an advantage to configure several NTP servers for improved robustness.

It is recommended that the primary NTP source be the closest core router or, alternatively, a server within the campus network. These should in turn obtain the time from a number of reliable sources, including UNINETT.

6.9 Other server functions in a switch

For general, important security reasons, all services which are not used in connection with a switch should be de-activated. These include finger, BOOTP, UDP Echo and HTTP (if not used).

6.10 Stacking

Some switches can be stacked to produce a “virtual chassis” with the stacking cable forming the backplane. This may call for a certain amount of configuration. Switches may also be stacked virtually, but only for the purpose of simplifying administration, in other words by providing a single IP address to administer a number of switches. This also calls for special configuration.

6.11 Remote console, console log

A facility for logging in to the console port of a switch is beneficial. This is not very realistic for edge switches and branch switches, but such an arrangement is recommended for core switches, i.e. especially those switches which also perform routing. This can also be achieved by connecting a serial port to a terminal server in the room, or a modem, or if necessary by connecting via an AUX port on another unit.

An even better solution is to provide a console server which logs everything which happens at the console. Again, this is only relevant in connection with the most critical equipment.

7 VLAN Configuration

7.1 Trunk configuration (VLAN tagging)

Trunk configuration (VLAN tagging) should use IEEE 802.1q (not ISL or other proprietary variants).

Trunk configuration shall not be based on autoconfiguration. Auto setup should be de-activated at all ports. For trunk ports, trunk configuration should be performed manually, as this enables a greater degree of control. It is considered extremely important from a security point of view that it should not be possible to change a random client port to a trunk port if the client attempts to do so.

One should consider whether to configure so as to restrict which VLANs are permitted to traverse a given trunk. Some products require this, while others do not. Although for reasons of simplicity of management it may be tempting to omit it, it should be pointed out that such a configuration provides an even greater degree of control.

7.2 Management configuration for VLAN (GVRP, VTP, etc.)

GVRP (GARP, Generic Attribute Registration Protocol, VLAN Registration Protocol) is a standard management configuration for VLAN using IEEE 802.1q trunks. Several suppliers support this protocol, though at present Cisco only supports it under CatOS. GVRP should be preferred over proprietary products such as Cisco's Virtual Trunking Protocol (VTP).

In any event, it is safest not to use such administration methods but instead to manually define the necessary VLAN for each switch. Supplier-specific properties connected with configuration may make this rather cumbersome.

If a VLAN administration method is used, this should be set up to be as secure as possible. This involves having full control over which ports are trunk ports, cf. Section 7.1, as well as using shared secrets, passwords, etc.

7.3 VLAN on unused ports / VLAN 1

The use of VLAN 1 is not recommended. It is recommended that a "dummy" VLAN be used for unused ports, so that incorrect connection or random connection does not result in a user obtaining access to a network for which he is not authorised.

Similarly, all non-trunk ports shall during the initial configuration be set to a VLAN value, either the VLAN which is to be used or to a "dummy" VLAN.

8 Spanning Tree Configuration

The spanning tree protocol must be run on the switches so that any physical loops are either consciously or unconsciously broken. Note that some switches support more VLANs than the number of spanning tree instances, and that this must be borne in mind during configuration.

8.1 Rapid spanning tree / MSTP

Standard spanning tree protocol has an unfavourably long convergence time. Note that this may also have a detrimental effect in situations where the design is loop-free, in other words in a pure tree structure. If one inadvertently creates loops, this will hinder traffic for an unnecessarily long time when standard spanning tree is implemented. One should therefore consider methods which provide more rapid convergence. IEEE 802.1w, also known as RSTP (Rapid Spanning Tree), is a standard which addresses this. If all the switches in a broadcast domain support RSTP, it should be used. MSTP should also be considered. MSTP enables multiple VLANs to be handled by the same spanning tree instance. MSTP also includes support for load sharing and more rapid convergence because redundant routes are theoretically operational, but since MSTP increases complexity one should weigh up the advantages and disadvantages.

8.2 Spanning tree root

The spanning tree root should be located on a core switch, as close to the router port as possible.

If possible, the root should be protected by a root guard.

8.3 PortFast

End-user ports should be configured with PortFast, so that a link is established before the full re-calculation of the spanning tree has been completed.

8.4 BPDU guard

If a switch supports this, it should be configured, and on all client ports – in other words those ports which are not configured with PortFast. The objective is to stop traffic if a switch is found to be present behind a client port.

9 Traffic Properties

9.1 Speed, duplex, autocrossing

All ports should be set to automatic. All clients should also be set to automatic, as this simplifies administration and leads to less likelihood of duplex conflicts.

If a given client does not support “auto” mode, the speed and duplex mode should be set manually. Routines must exist for tidying up when the machine in question is no longer behind the port.

One should be particularly careful in cases of auto-configuration where the duplex mode ends at half duplex. This often indicates a duplex conflict because of a non-auto configuration on the client side.

Some ports support autocrossing, and in some cases this must be configured explicitly.

9.2 Jumbo frames

Ports which support jumbo frames should be configured to use them. Jumbo frames result in an increase in MTU from 1500 bytes to 9000 bytes, which improves the transmission capacity of gigabit Ethernet, especially over long distances.

9.3 Bundling of ports (ether channel) /load balancing

In certain cases, it may be useful to double or multiply the capacity of a link by combining multiple fast Ethernet or gigabit Ethernet ports. Cisco’s proprietary system is known as EtherChannel. IEEE 803.ad is a standard for such link aggregation.

9.4 Traffic management / Quality of Service (QoS)

Quality of service functions may be configured according to needs, including support for different service classes, policing and shaping.

9.5 Power over Ethernet

If a switch port is to be connected to an IP telephone, a base station or some other unit based on power supply over the network cable, this must be configured. Conversely it will be appropriate to de-activate this if it is not wanted.

9.6 Protection of the control plane

To protect the CPU (as is particularly relevant on core switches), measures should be adopted to control and safeguard resource utilisation and access to it.

9.7 Physical link monitoring

If a switch supports mechanisms for monitoring the physical cable to which a given port is connected, such functions should be activated.

10 Multicast snooping

Switches must have support for IGMP snooping, both Version 2 and Version 3. Version 3 is important for handling SSM (single source multicast), which is becoming increasingly widespread. IGMP snooping should be activated on all ports.

11 Security Functions

11.1 Port security

The port security functions can be used to enable better access control to a given switch port. This allows only a certain number of machines (MAC addresses) behind a given port. The configuration should be such that authorised machines still have network access after any additional machines are connected. Only the additional machines are blocked. The function is recommended especially in connection with printers in open areas, so that these switch ports are not misused.

As a minimum requirement, all client ports should be configured with a high value which exceeds practical usage, so as to prevent flooding of the CAM table. Note that network ports (ports connecting to other network equipment) must not have this type of configuration.

11.2 IEEE 802.1X

IEEE 802.1X provides better control over who accesses the network. The disadvantage of this is that it requires more of the client, which must have configured support. Moreover, the user must log in each time the network is accessed.

IEEE 802.1X is recommended especially for wireless networks, but can also be used effectively on a fixed network. One can choose to implement it for individual user groups, such as student villages.

11.3 Traffic storm control

The port should be configured so that broadcast traffic is blocked when its volume exceeds a pre-defined acceptable threshold (e.g. 10 %).

11.4 DHCP snooping

DHCP snooping should be configured for edge switches (provided it is supported by the switch). The objective is to prevent incorrectly configured clients from behaving as DHCP servers and hence assigning false IP addresses to other clients. This has become a problem and can be avoided by implementing DHCP snooping with its associated blocking function. It is important that this function is only implemented in client ports and not on trunk or network ports.

11.5 IP source guard / dynamic IP lockdown

This is a mechanism which prevents forgery of IP addresses from the client machine. Only the IP address assigned to the client by DHCP or any statically registered address can be used behind the port.

If a switch supports this function, it is recommended that it be actuated on client ports. The function may require that DHCP snooping is also being used.

11.6 Dynamic ARP inspection

This mechanism protects against “man-in-the-middle” attacks which send false ARP packets pretending to behave as a router. If the switch knows which IP addresses should belong behind which ports it can effectively block attempts at pretending to be somebody else by way of ARP. This function should definitely be considered, but may require that DHCP snooping is also in use.

11.7 Port unicast and multicast flood blocking

If packets are sent to new, false MAC addresses, these will always be sent out to all the ports on a switch. A deliberate attack may hence degrade performance for the entire environment behind the port. This may be prevented by configuring this function. If a switch supports this property, one should consider actuating it on all client ports.

11.8 MAC address notification

This is a mechanism which sends an SNMP trap when a new MAC address is discovered or aged out on a switch. If the SNMP trap receiver is capable of interpreting it, an accurate picture of the client machines in the network can be obtained. Such mapping may also be achieved by performing regular SNMP polling of the switches, although this provides a somewhat cruder picture. If a switch supports this function, it should be activated.

12 Useful functions for day-to-day operations

12.1 Port mirroring

It is useful to configure port mirroring when needed. This function sends a copy of all traffic from one port out to another port. On the monitoring port one can analyse the traffic using, for example, a sniffer or tcpdump.

12.2 Blocking a MAC address

A MAC address can be effectively blocked by configuration of a switch. An alternative approximation is to use a network management system with support for machine blocking. It is also possible to block an IP address with a Layer 3 filter.

12.3 Static binding of a MAC address to a port

The same function can be activated using port security, but it is possible to define static bridge table entries if desired.