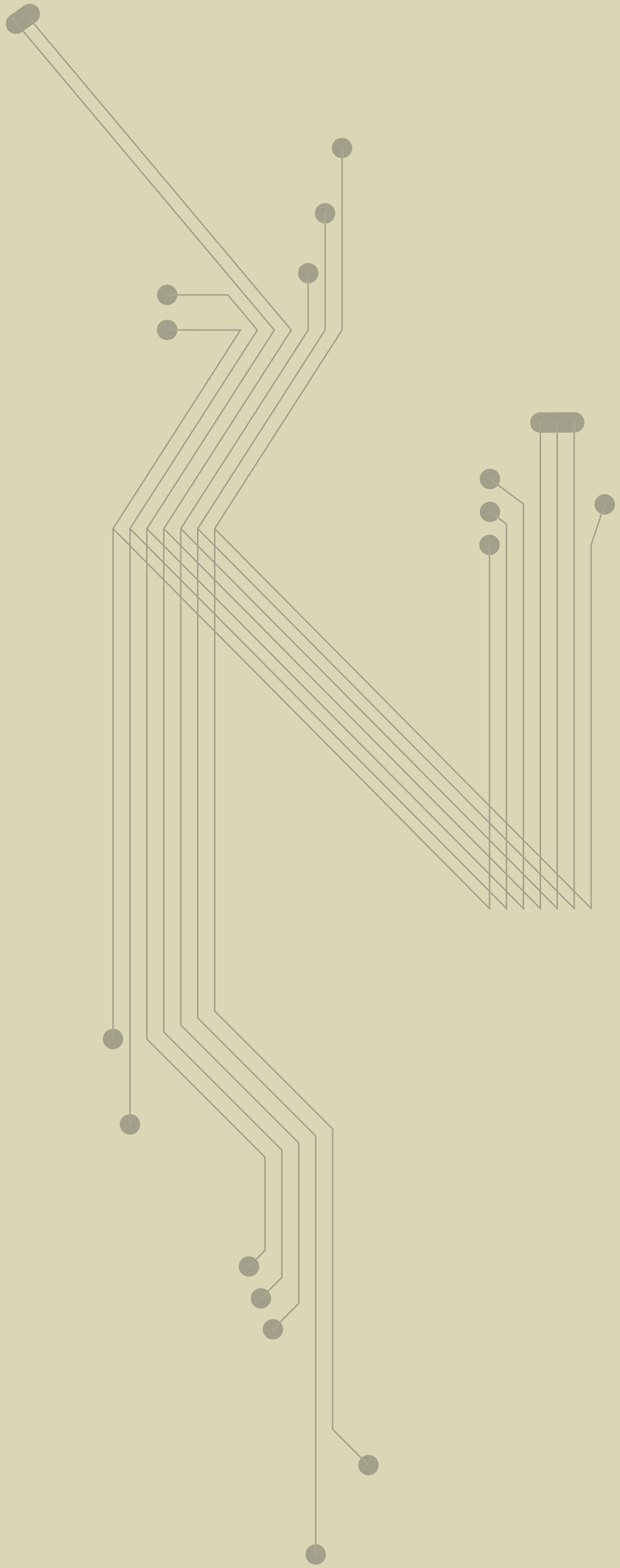


S4

Teleste S4 Access Switch

Secure Subscriber Connections in an Open-Access FttH Networking Topology

Background

To safely provide secure subscriber connections in an open-access FTTH networking topology where broadband services are made available on different L2 VLANs sets new and great demands on the security features found in network access switches operating as high-performance Ethernet aggregators.

Neighbours subscribing to the same VLAN service are allowed, by the nature of the broadcast media, to communicate with each other, but communication needs to be controlled by stringent security features found in upstream access switches to ensure subscriber-security and integrity.

A hacker, being locally connected or who may have gained control of a local connected computer, can exploit and compromise a network utilizing the lack of security in a protocol that is required for TCP/IP networking to conduct.

Teleste FTTx S4 Access Switch includes a vast portfolio of security mechanisms some of its qualities are explained beneath.

Preventing creation of deliberate illegal traffic flows

ARP-spoofing/poisoning: In a shared broadcast media like an Ethernet VLAN information is distributed to multiple entities, a hacker can e.g. create false ARP reply packets that can change the flow of traffic which can facilitate in eavesdropping of IP telephony calls as well as to monitor and observe private usernames and passwords for Webmail, Online Banking and similar services. It is of great importance to detect and prevent ARP-spoofing/poisoning attempts by implementing a dynamic ARP inspection feature since the communication model relies heavily on trust and assumes that all ARP reply traffic is legitimate. The S4 Access Switch imposes strict control over what ARP packets are allowed into the network.

IPv6: Ability to block between subscriber ports ICMPv6 Router Advertisement messages. Today certain client operating systems, such as Windows Vista and Windows 7, have IPv6 auto configuration enabled by default, which means it's possible for a hacker to redirect subscriber traffic to pass his/her own computer assisting in performing a Man in the Middle attack. The S4 Access Switch can block ICMPv6 Router Advertisement messages.

Controlled IP assignment and IP source guard abilities

The S4 Access Switch supports monitored client IP configuration over DHCP using its DHCP snooping agent. When the DHCP snooping feature is enabled it enforces hardened network security that provides for:

- Only authorized DHCP servers are available
- Subscribers can only use the IP addresses assigned to them to communicate, preventing illegal use of setting fixed IP addresses
- Assist in tracking physical location of hosts
- Automatic ACL's are created in the S4 giving communication credentials based on the DHCP assignments, delivers IP source guard abilities and prevents IP hijacking attacks
- A real time snooping database keeps track of assignments and lease times

The S4 supports also the concept of monitored manual IP assignment – i.e. setting fixed IP addresses at subscriber devices. Also for this type of assignment scheme, IP source guard abilities are met, only IP addresses configured for an interface is allowed to communicate.

Controlled traffic flows by means of access control lists

The S4 switch provides the ability to tailor make policies controlling inbound and outbound subscriber traffic flows. Implementing well designed ACL's will control and restrict availability of certain network resources, protecting the infrastructure as well as preventing malicious subscribers from injecting illegal unwanted traffic into the network. Filtering capabilities can be implemented for L2/L3/L4 traffic; the feature operates distributed in hardware and will not oppress CPU normal operation.

Port security and MAC locking

The S4 allows for configuring a secure subscriber port, i.e. allowing only certain MAC addresses or a certain amount of MAC addresses to communicate over a certain interface.

Increased flexibility is obtained due to the support of wild card characters in filter design, e.g. the three most significant octets of a MAC address (Organizationally Unique Identifier, OUI) may be specified in a filtering rule. For the latter three octets - wild card can be used. The quality can e.g. be used for preventing set-top box mobility and it can be mapped to a VLAN.

Traceability

Option-82: If enabling the Option-82 feature the S4 will automatically manage the sub-options fields; Agent Remote ID and Agent Circuit ID. Supplying information about DHCP traffic such as from which S4 the traffic was switched as well as information defining what S4 subscriber port and what service VLAN the traffic was passed on. This will facilitate for the service provider to track and map IP address assignment to individual subscribers. The feature fulfils country specific legal demands.

SKA-certifierad
SSNF
Säker-Kund-Anslutning

Configuring subscriber security

Introduction

The objective of the configuration example is to illustrate the configuration needed for a network provider to safely deliver secure subscriber connections in an open-access FTTH networking topology, i.e. where neighbours may subscribe to the same VLAN service, and by the nature of the broadcast media are allowed to communicate with each other.

Scope

The configuration example makes use of the assumptions that follows:

- Different broadband services are arranged and made available in the target network on separate service VLANs as depicted in figure 1.
- Subscribers can only use the IP addresses assigned.
- The configuration example enables the ability of detecting and preventing ARP-spoofing/poisoning attempts by implementing a dynamic ARP inspection feature. Figure 2 illustrates an example of how an ARP-spoofing/poisoning attempt may be accomplished.
- The configuration shall only allow authorized DHCP servers residing at either uplink port A or B and shall completely block all DHCP server traffic arriving at subscriber interfaces.
- Only allow monitored client IP configuration over DHCP using S4 DHCP snooping agent.
- Subscribers shall only be able to use the IP addresses assigned to them to communicate; configuration shall prevent illegal use of setting fixed IP addresses.
- The configuration settings shall assist in tracking physical location of hosts, i.e. by enabling Option-82 support.
- The configuration will result in that automatic ACL's are created in the S4 giving client communication credentials based on the DHCP assignments; it will deliver IP source guard abilities and prevents IP hijacking attacks.

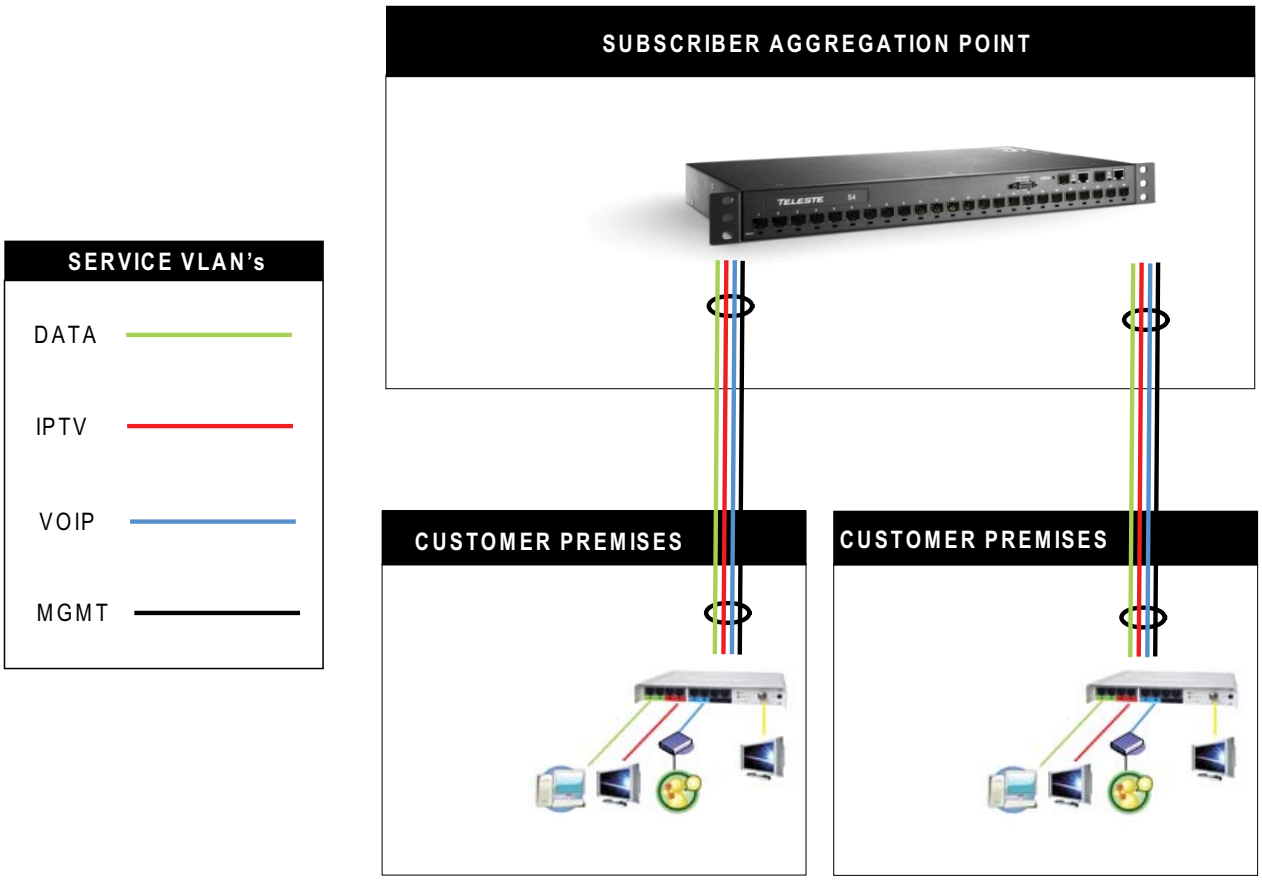

Figure 1. Different services arranged and offered on different VLANs

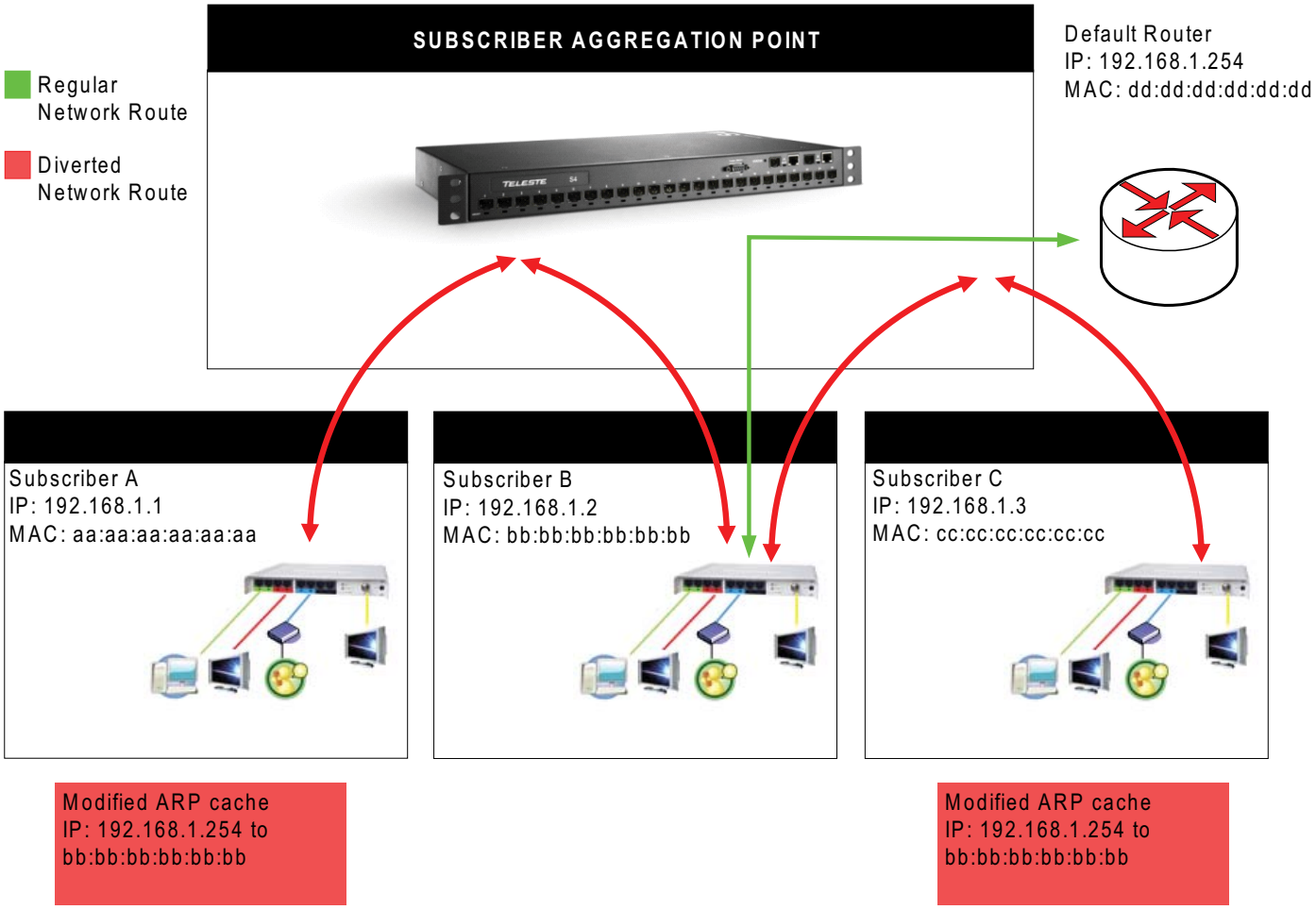

Figure 2. A setup where an Access Switch has dynamic ARP inspection disabled or is missing this feature. Subscriber B has successfully poisoned other subscribers ARP cache and diverted normal traffic flow.

Configuration Example

Follow the steps below to carry out a configuration according to the assumptions made earlier:

1. Begin by globally enable 'Subscriber Security' on the S4 switch.
S4> subscr-security on
The command enables subscriber security globally in the S4 switch; it operates in combination with the 'if-subscr-security' command and together they provide the ability of detecting and preventing ARP-spoofing/poisoning attempts by implementing dynamic ARP inspection.

2. Enable local interface subscriber security for subscriber ports 1-24
S4>if-subscr-security 1-24 1

3. Enable DHCP snooping
S4> dhcp-snooping on
Enables monitored client IP configuration over DHCP. The DHCP snooping agent dynamically builds and maintains a DHCP snooping database. Subscribers can only use the IP addresses assigned to them to communicate, preventing illegal use of setting fixed IP addresses.

4. Enable DHCP Option-82. The feature assists in traceability and tracking of physical location of subscribers.
S4>dhcp-option-82 on
The command enables the insertion of DHCP Option-82 information into the DHCP options field, when forwarding subscriber originated DHCP packets to a DHCP server. In the opposite direction the switch will remove DHCP Option-82 information in DHCP reply packets destined for subscriber ports.

S4 inserts the following Option-82 information:
- Remote ID.
- Circuit ID.
This specifies the subscriber port and the VLAN ID that the DHCP packet was received on

5. Next, specify what Option-82 Remote ID insertion mode to use. Either the switch can be recognized by its IP address or its MAC address. To specify the use of the IP address issue the below command.
S4> option-82-type 1

6. Specify DHCP untrusted and trusted ports. Subscriber ports 1-24 is set to be untrusted and uplink ports to be trusted.
S4>dhcp-trust 1-24 0
S4>dhcp-trust A 1
S4>dhcp-trust B 1

When DHCP snooping is enabled the switch will only forward captured DHCP packets onto trusted ports that connects to trusted network elements, i.e. trusted DHCP servers.

7. Set the maximum number of IP address assignments allowed by the snooping binding database for a particular subscriber port. The example sets a max. assignment of two IP addresses allowed per subscriber port.
S4>dhcp-max-count 1-24 2
When the limit is reached, further assignments are prevented.

8. Finish by saving the configuration.
S4>nvsave
nvsave successfully.

9. The configuration can be verified by issuing the following command:
S4>show-subscr-security

Current global subscr. security: On
Current per port subscr. security:
Port 1: On | Port 2: On | Port 3: On | Port 4: On | Port 5: On | Port 6: On | Port 7: On | Port 8: On | Port 9: On | Port 10: On | Port 11: On | Port 12: On | Port 13: On |Port 14: On | Port 15: On | Port 16: On | Port 17: On | Port 18: On | Port 19: On |Port 20: On | Port 21: On | Port 22: On | Port 23: On | Port 24
: On | Port A: Off | Port B: Off |

Current DHCP snooping: On
Current DHCP option 82: On
Current per port DHCP Trust:
Port 1: Off | Port 2: Off | Port 3: Off | Port 4: Off | Port 5: Off | Port 6: Off | Port 7: Off | Port 8: Off | Port 9: Off | Port 10: Off | Port 11: Off | Port 12: Off | Port 13: Off | Port 14: Off | Port 15: Off | Port 16: Off | Port 17: Off | Port 18: Off | Port 19: Off | Port 20: Off | Port 21: Off | Port 22: Off | Port 23: Off | Port 24: Off | Port A: On | Port B: On |

Current per port DHCP current/max count:
Port 1: 0/2 | Port 2: 0/2 | Port 3: 0/2 | Port 4: 0/2 | Port 5: 0/2 | Port 6: 0/
2 | Port 7: 0/2 | Port 8: 0/2 | Port 9: 0/2 | Port 10: 0/2 | Port 11: 0/2 | Port
12: 0/2 | Port 13: 0/2 | Port 14: 0/2 | Port 15: 0/2 | Port 16: 0/2 | Port 17:
0/2 | Port 18: 0/2 | Port 19: 0/2 | Port 20: 0/2 | Port 21: 0/2 | Port 22: 0/2 |
Port 23: 0/2 | Port 24: 0/2 |

DHCP bound IP address:

Fixed IP address set manually:
Port 1, Name: , Allowed fixed IP address:
Port 2, Name: , Allowed fixed IP address:
Port 3, Name: , Allowed fixed IP address:
Port 4, Name: , Allowed fixed IP address:
Port 5, Name: , Allowed fixed IP address:
Port 6, Name: , Allowed fixed IP address:
Port 7, Name: , Allowed fixed IP address:
Port 8, Name: , Allowed fixed IP address:
Port 9, Name: , Allowed fixed IP address:
Port 10, Name: , Allowed fixed IP address:
Port 11, Name: , Allowed fixed IP address:
Port 12, Name: , Allowed fixed IP address:
Port 13, Name: , Allowed fixed IP address:
Port 14, Name: , Allowed fixed IP address:
Port 15, Name: , Allowed fixed IP address:

Port 16, Name: , Allowed fixed IP address:
Port 17, Name: , Allowed fixed IP address:
Port 18, Name: , Allowed fixed IP address:
Port 19, Name: , Allowed fixed IP address:
Port 20, Name: , Allowed fixed IP address:
Port 21, Name: , Allowed fixed IP address:
Port 22, Name: , Allowed fixed IP address:
Port 23, Name: , Allowed fixed IP address:
Port 24, Name: , Allowed fixed IP address:
Port A, Name: Giga 1, Allowed fixed IP address:
Port B, Name: Giga 2, Allowed fixed IP address:

Teleste, an international technology group founded in 1954, is specialized in broadband video and data communication systems and services. The group is divided into two strategic business areas: Broadband Cable Networks and Video Networks. Broadband Cable Networks consists of two Business Units that serve cable operators and a major part of its business activities are handled through direct customer contact. Video Networks Business Unit supplies solutions for optical signal transmission and video network management software solutions for video surveillance and a major part of its business is handled through system integrators. The business Units are among the leading providers in their market areas and are globally recognized for their know-how and ability to produce technically cutting edge solutions year after year. In 2006 the group's net sales in continuing business totalled EUR 101.8 million, and the group employed 621 persons at the year-end. The company has approximately 30 offices worldwide. Close to 90% of Teleste's net sales are generated outside Finland. The company is listed on the main list of Helsinki Exchanges.

Teleste Corporation

P.O.Box 323, FI-20101 Turku, Finland
Phone +358 (0)2 2605 611
Fax +358 (0)2 2605 928
E-mail info.bcn@teleste.com
www.teleste.com

WP_1109_54