DO NOT REPRINT
© FORTINET
Passdumps.com



FortiSwitch

Study Guide

for FortiSwitch 7.2

FORTINET®

Training Institute

Vouchers & Dumps are Available | WhatsApp +201224665523

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

2/14/2023

Vouchers & Dumps are Available | WhatsApp +201224560923

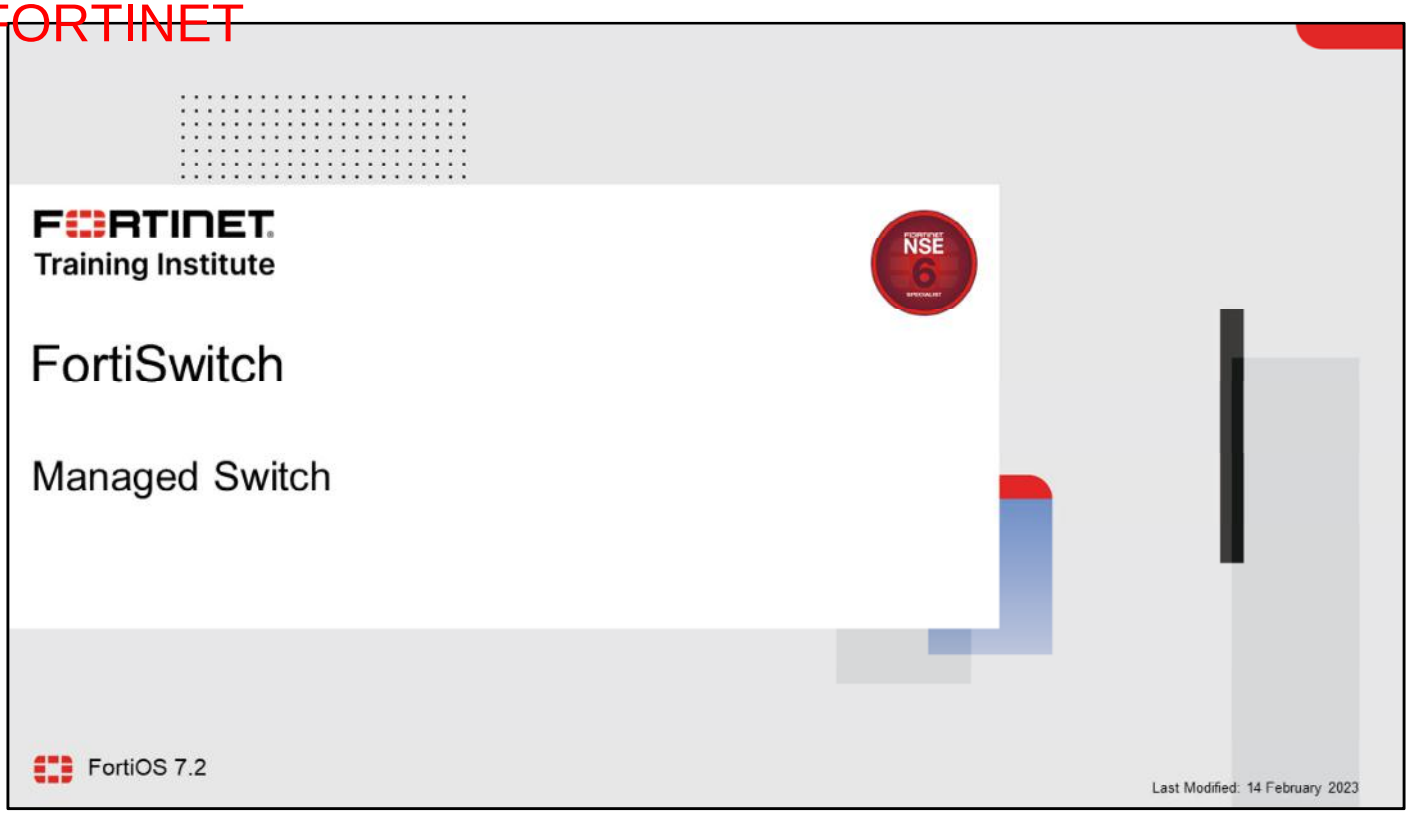
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Managed Switch **4**
02 Switch Fundamentals **69**
03 Layer 2 Design **140**
04 Layer 2 Security **207**
05 Advanced Features **249**
06 Monitoring **306**
07 Standalone Switch **329**
08 Troubleshooting **397**

Vouchers & Dumps are Available | WhatsApp +201224560923

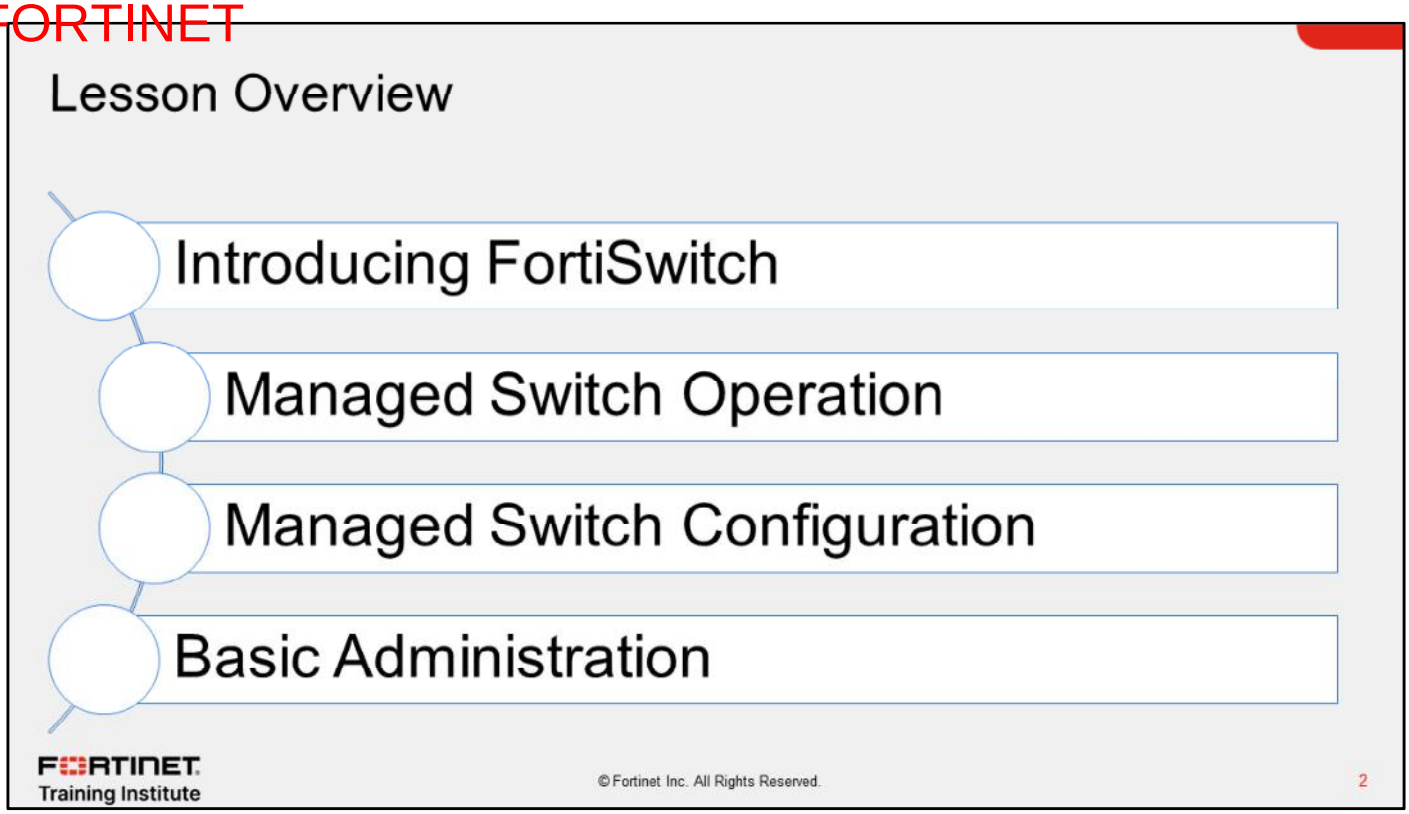
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSwitch essentials, focusing on the managed switch mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

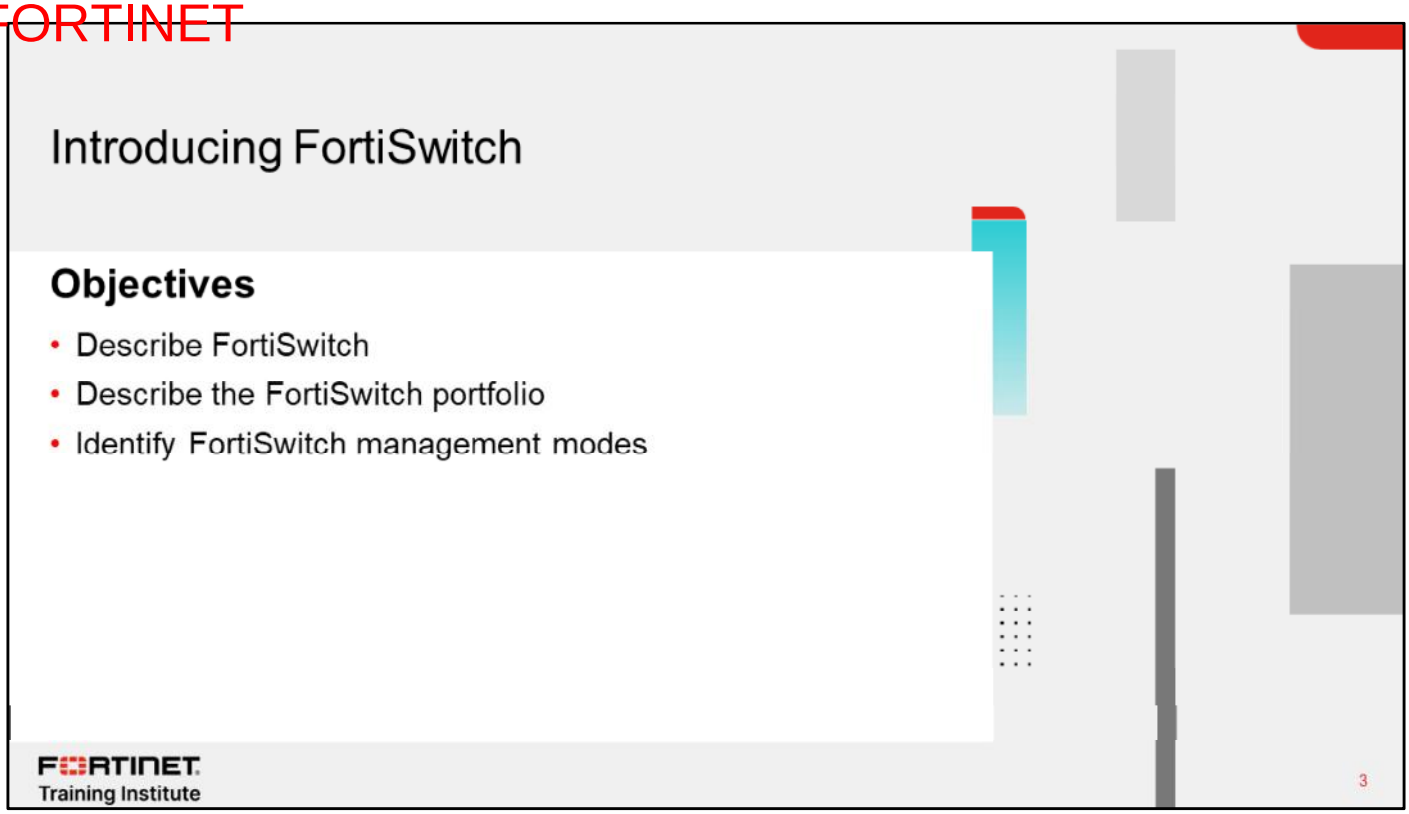
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

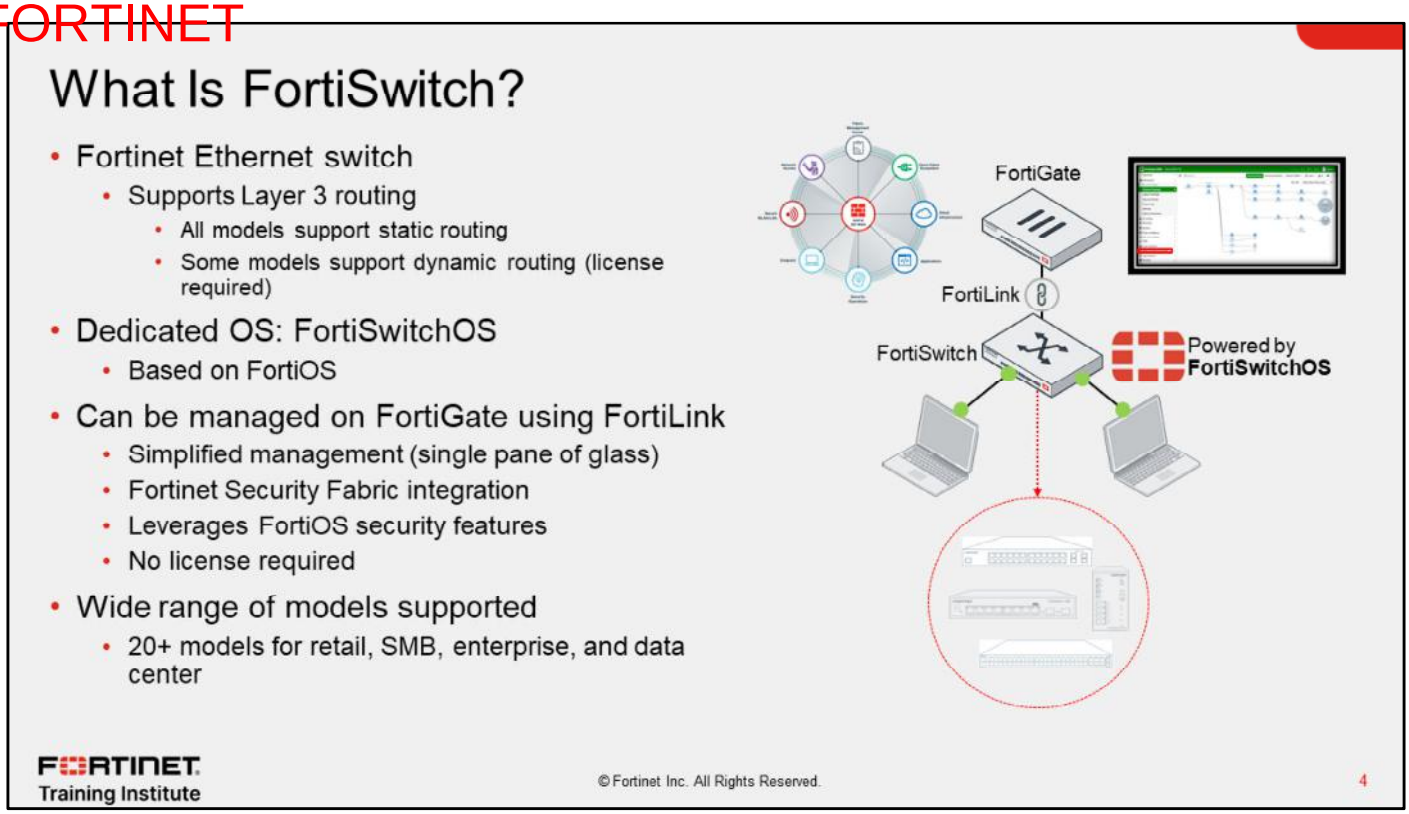


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiSwitch, you should be able to identify FortiSwitch models and management modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiSwitch is Fortinet Ethernet switch device. Like any other Ethernet switch, it operates at Layer 2 of the OSI model by forwarding Ethernet frames based on the frame's destination MAC address and the contents of the switch's MAC address table. Layer 3 static routing is also supported on all models, and dynamic routing on some models. The models that support dynamic routing require an advanced features license. You will learn more about FortiSwitch routing features in another lesson.

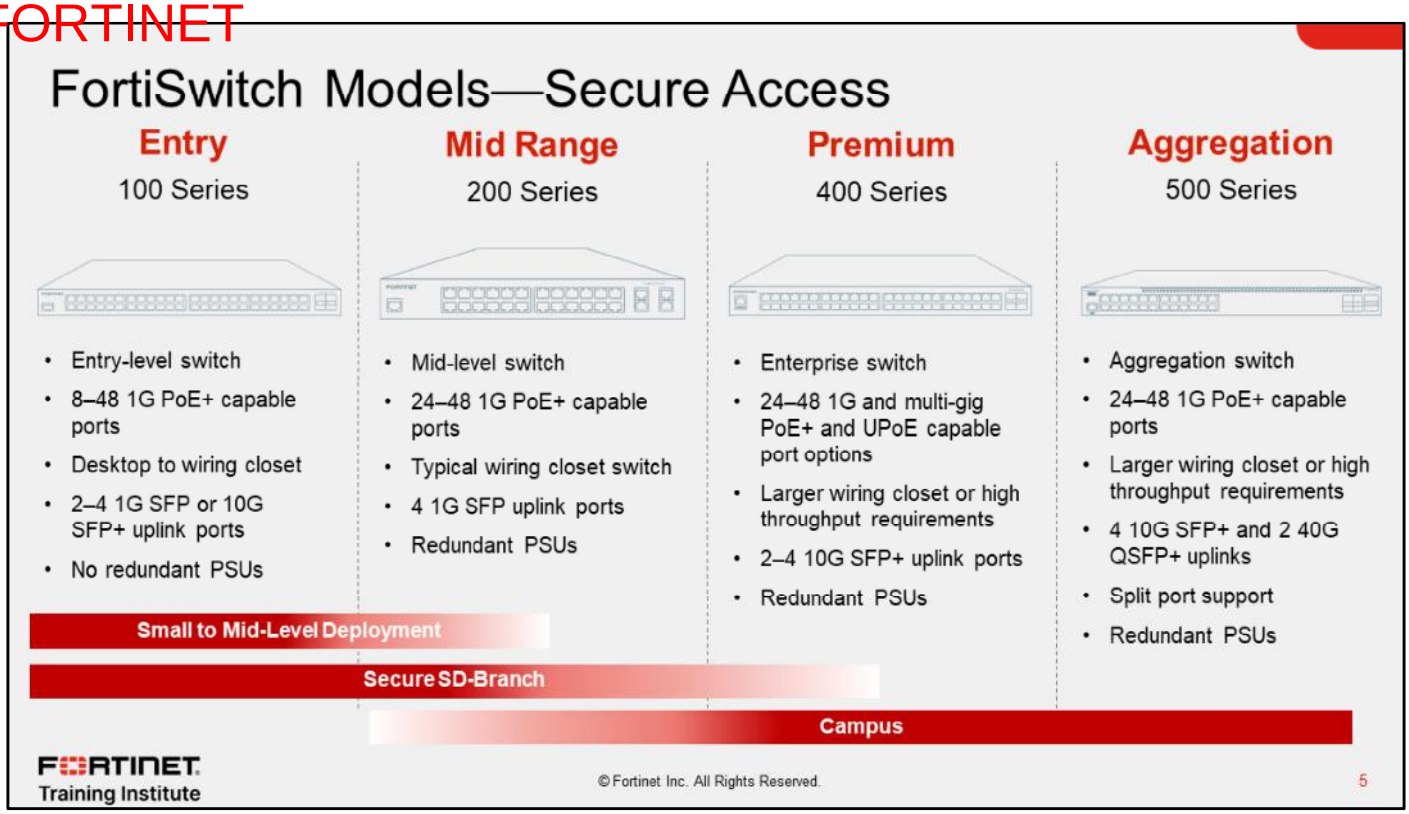
FortiSwitch runs its own operating system: FortiSwitchOS. FortiSwitchOS is based on the FortiOS kernel and several FortiOS user-space applications. Some of these applications have been customized to meet FortiSwitchOS requirements. Because FortiSwitchOS is based on FortiOS, most of the FortiSwitchOS configuration, troubleshooting, CLI commands, and output, are very similar to FortiOS, and in some cases, identical. As a result, an administrator with experience in FortiOS will find FortiSwitchOS very familiar, which will then shorten the learning curve considerably.

You can manage FortiSwitch on FortiGate using FortiLink. This is the most common deployment, and it does not require an additional license. When you manage FortiSwitch on FortiGate, you simplify management by using the FortiGate GUI and CLI to manage both devices. In addition, when managed on FortiGate, FortiSwitch integrates with the Fortinet Security Fabric, which enables FortiSwitch to work together with FortiGate and other products, such as FortiManager, FortiAnalyzer, and FortiAuthenticator, to enhance LAN edge security, deployment, configuration, and troubleshooting.

There are more than 20 FortiSwitch models to choose from. The range of models available target different business sizes and use cases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiSwitch portfolio classifies FortiSwitch models based on their use case: secure access, data center, and rugged. This slide describes the FortiSwitch secure access series.

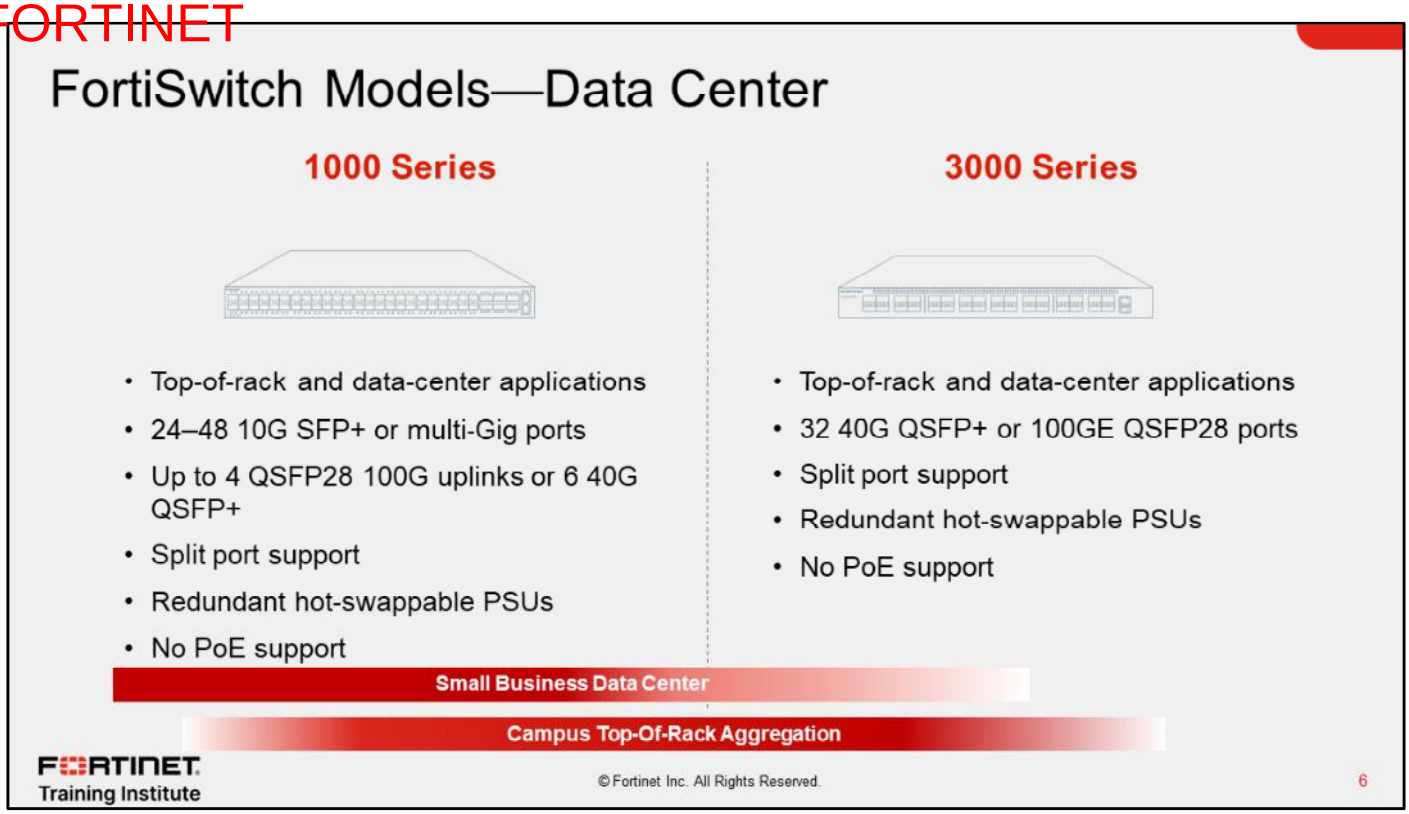
The secure access series is designed with endpoint connectivity in mind. The different models enable businesses to scale from the smallest retail setting to the data center. There are four families: the 100 series, 200 series, 400 series, and 500 series. Uplink capacity is the most distinguishable difference between each series, starting with the 100 series with two 1G uplinks and ending with the 500 series with two 40G uplinks.

Usually, choosing the right secure access switch model is determined by the network traffic demands. In small and remote sites, deploying 100 and 200 series switches is generally more than sufficient. However, in larger networks with higher throughput requirements that demand more uplink capacity, deploying 400- and 500-series switches may be more convenient.

In terms of power delivery, all series offer models supporting power over Ethernet+ (PoE+) ports, but only the 400 series offers models supporting universal PoE (UPoE).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The data-center model switches are designed to perform as top-of-rack distribution switches in data-center deployments. The 1000 series offers higher port density, while the 3000 series offers higher throughput. In both series, you can split 40G and 100G ports into multiple lower-speed ports to achieve higher port density and aggregate more devices. In addition, both switches offer redundant hot-swappable power supplies, but no PoE support. The lack of PoE support should not represent a constraint because the switches are not really meant to connect endpoints, but rather to aggregate traffic coming from access switches.

You can combine these switches with the secure access line to deploy a FortiGate managed switch stack that can scale as your network grows.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSwitch Models—Rugged



112D-POE

- 8 1G RJ45 PoE+ capable ports
- 4 1G SFP ports



124D Switch

- 16 1G RJ45 ports and 4 1G SFP ports
- 8 shared media interfaces (GE RJ45 / GE SFP slots)

Passive cooling, no fans or moving parts
Redundant power inputs
IP30 rating protection

FORTINET Training Institute

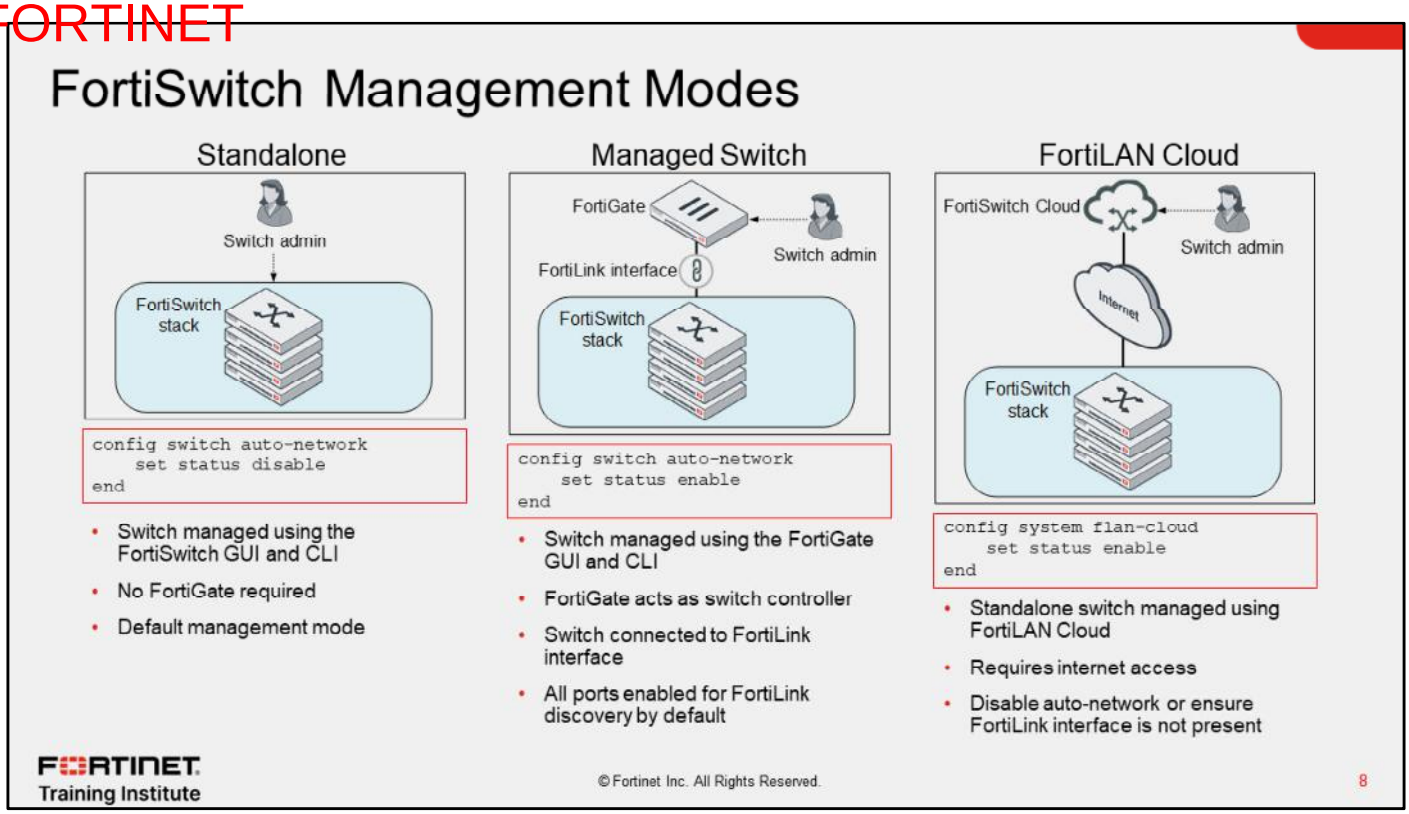
© Fortinet Inc. All Rights Reserved.

7

The rugged model switches are designed to withstand more challenging environments, such as those found in operational technology (OT) networks and other critical infrastructure where dust and other harsh conditions may be present. The switches feature a passive cooling mechanism and no fans or moving parts. The switches also offer redundant power inputs and are built with an IP30 protection rating.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can deploy FortiSwitch as a standalone switch or as a managed switch.

The factory default management mode on FortiSwitch is standalone, also known as local mode. When in standalone management mode, you can manage the switch through the FortiSwitch GUI and CLI interfaces, or from FortiLAN Cloud. FortiLAN Cloud is a management as a service (MaaS) solution that provides centralized discovery, visibility, and configuration for standalone FortiSwitch devices. FortiLAN Cloud requires every switch to have internet access.

When deployed as a managed switch, the switch is controlled by FortiGate, which acts as the switch controller and uses its FortiLink interface to communicate with the switch. Under this mode, you manage the switch from FortiGate. The managed switch mode is also known as FortiLink mode. This lesson covers the managed switch mode only.

This slide also shows the FortiSwitchOS CLI settings that control the switch management mode. By default, the switch is operating in local mode, however the `switch auto-network` configuration option is set to `enable`. The switch is therefore operating in standalone mode and will attempt to discover a FortiLink interface on FortiGate. You can alter the FortiSwitch automatic discovery behavior by setting the `switch auto-network` setting to `disable` the on the CLI. If you also want to manage your standalone switch from FortiLAN Cloud, ensure that the feature is enabled under `config system flan-cloud` (it is disabled by default).

Note that unlike in previous FortiSwitchOS firmware versions, when you change the management mode of FortiSwitch, the switch does not reboot. Finally, unless otherwise stated, all references in this lesson are for managed switch mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the name of the firmware running on FortiSwitch?
   - A. FortiOS
   - ✓ B. FortiSwitchOS

2. What management mode enables you to manage FortiSwitch on FortiGate?
   - ✓ A. Managed switch
   - B. FortiLAN Cloud

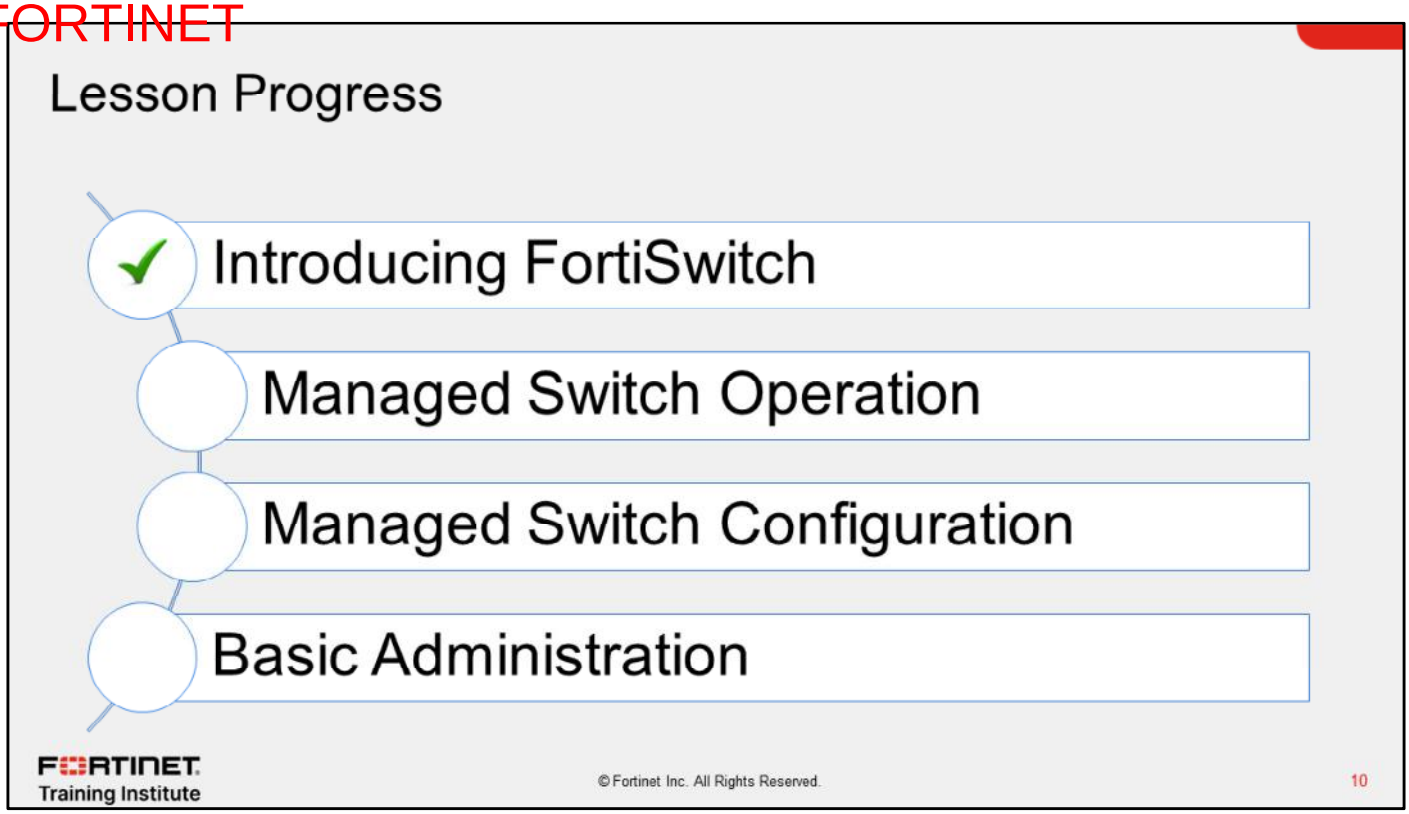
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

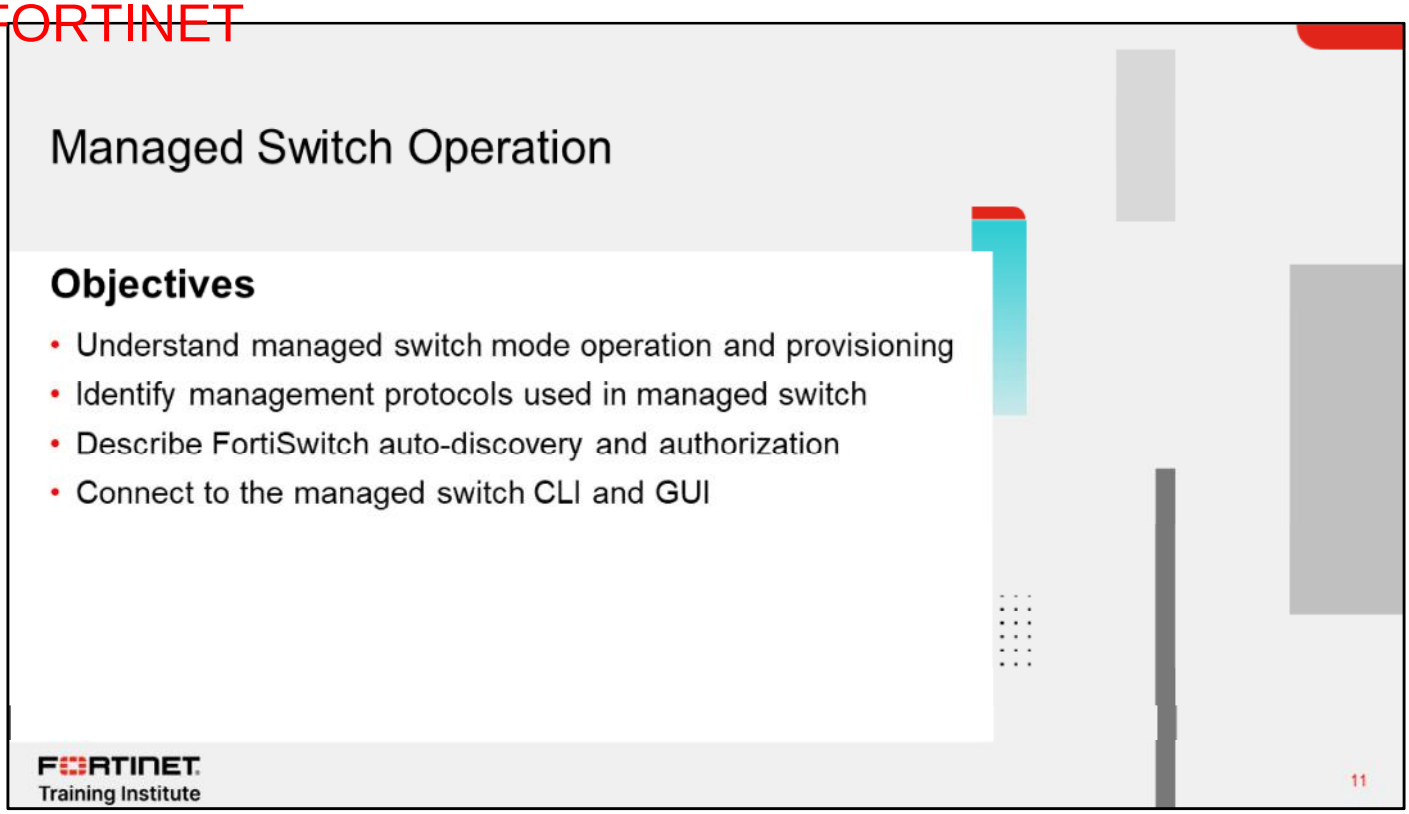


Good job! You now understand FortiSwitch basics.

Now, you will learn about managed switch operation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

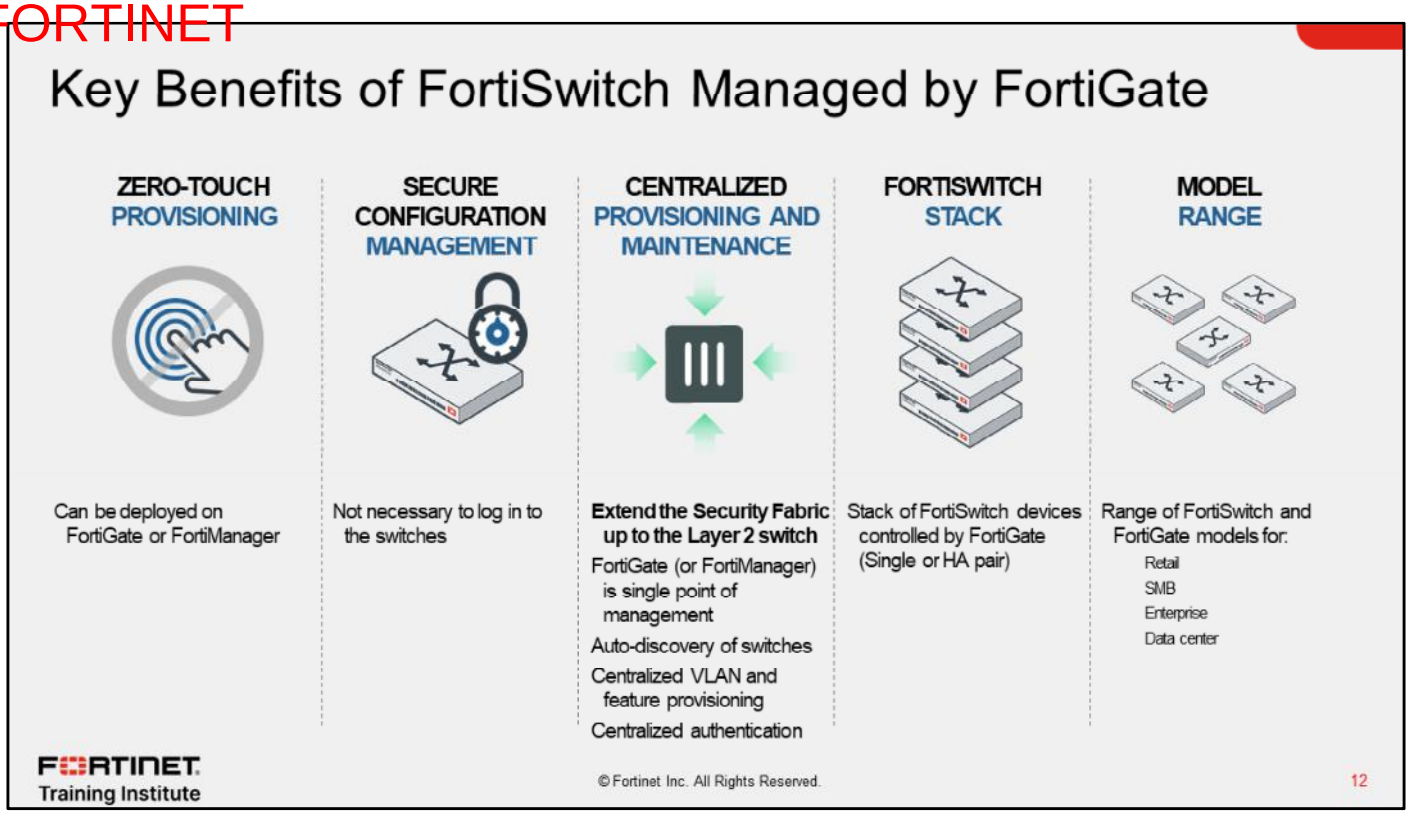


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managed switch operation, you should be able to understand how managed switch works, the role of the different management protocols involved, and the FortiSwitch auto-discovery and authorization process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

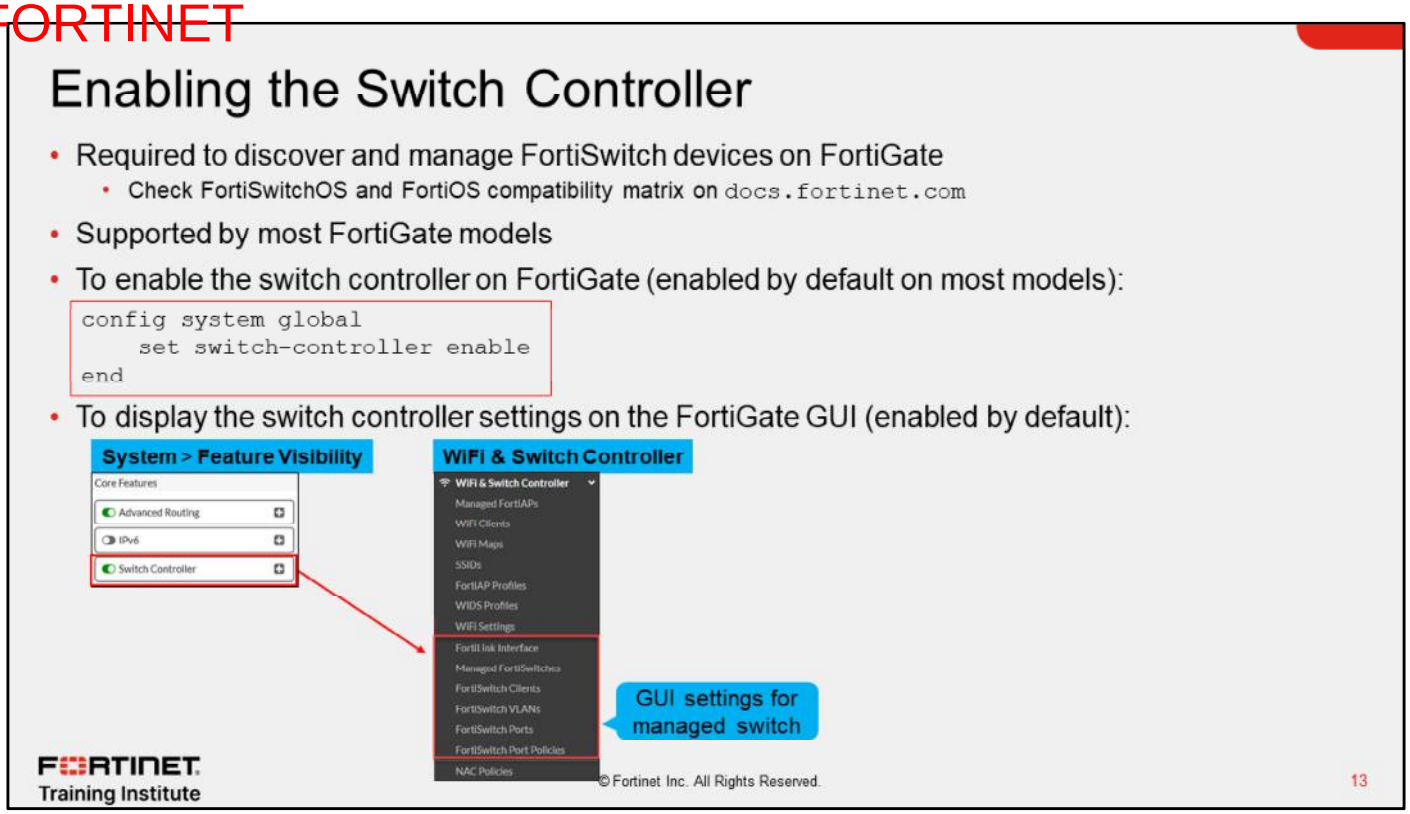


Managing FortiSwitch devices using FortiGate offers the following important key benefits:

- Zero-touch provisioning: Administrators only need to connect FortiSwitch to a FortiGate interface that has FortiLink enabled. FortiGate automatically discovers and provisions FortiSwitch. If FortiManager is used, you can also achieve zero-touch provisioning by configuring the FortiGate settings on FortiManager.
- Secure configuration management: All FortiSwitch management is done on the FortiGate GUI and CLI, or on FortiManager if used. Administrators are not required to log in to FortiSwitch.
- Centralized provisioning and maintenance: FortiSwitch becomes an extension of FortiGate. The way you configure firewall policies using FortiSwitch VLANs is the same as the way you do it for FortiGate VLANs. Authentication and authorization are also handled centrally on FortiGate or FortiManager.
- FortiSwitch stack: FortiGate can manage multiple FortiSwitch devices stacked in different ways to offer scalability and redundancy.
- Model range: There are different sizes of FortiGate and FortiSwitch devices to accommodate the needs of everyone from retail and SMB customers up to data centers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Before you can manage your FortiSwitch stack on FortiGate, you must ensure the switch controller feature is enabled on FortiGate, so FortiGate can discover and manage connected FortiSwitch devices. In addition, you must make sure the FortiSwitchOS version of your switch is compatible with the FortiOS version of your FortiGate. You can check the FortiSwitchOS and FortiOS compatibility matrix on `docs.fortinet.com`.

By default, the switch controller feature is enabled on most FortiGate models. In FortiGate VM models, however, it is not enabled by default, but you can enable it by running the CLI commands shown on this slide.

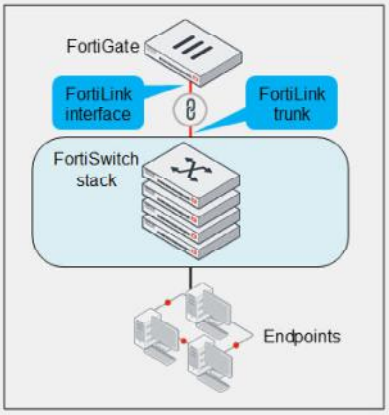
After you enable the switch controller feature, the related switch controller settings are shown on the GUI under the **WiFi & Switch Controller** section. If the GUI settings are not shown, make sure that the **Switch Controller** feature is enabled on the **Feature Visibility** page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Managed Switch Overview

- FortiGate uses a dedicated FortiLink interface to:
  - Manage the FortiSwitch stack
  - Process inter-VLAN and internet traffic from users, and traffic destined to the firewall
- A managed switch connects directly or indirectly (stacked) to a FortiLink interface
- Various network topologies supported
  - Multiple FortiLink interfaces can be created on multiple VDOMs
  - FortiGate can be in standalone, HA A-P, or HA A-A mode
  - VDOM controlling switches must be in NAT mode



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

To manage FortiSwitch on FortiGate, the switch must be connected directly or indirectly to a FortiLink interface on FortiGate. The FortiSwitch side of the FortiLink interface is called the *FortiLink trunk*. You will learn more about FortiSwitch trunks in another lesson.

A group of managed switches that are connected to the same FortiLink interface is called a FortiSwitch stack. There are multiple ways you can connect the switches together and to FortiGate. You will learn about the different network topologies supported in another lesson.

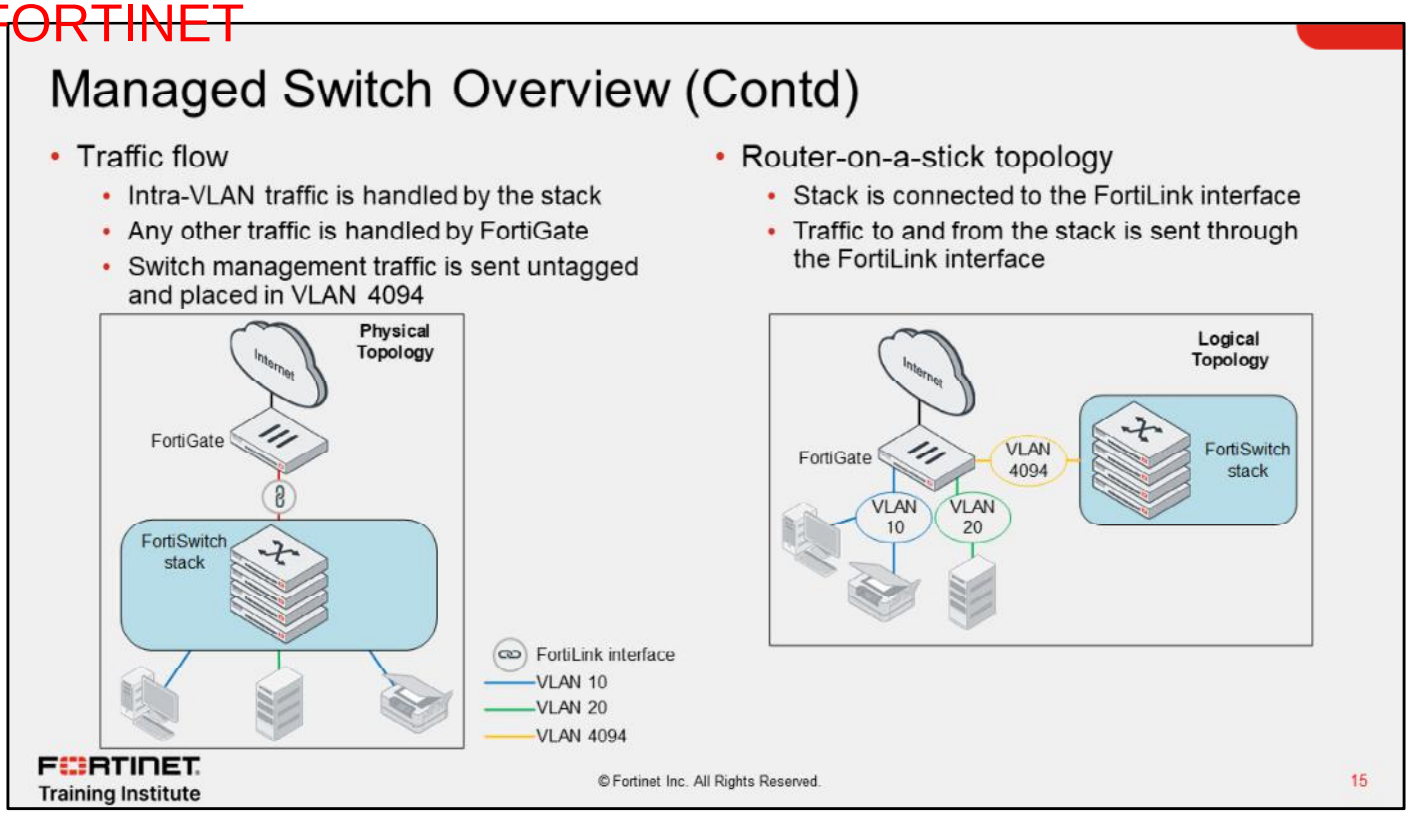
Switch management traffic between FortiGate and the stack travels through the FortiLink interface. In addition, user inter-VLAN and internet traffic from endpoints connected to the FortiSwitch stack, as well as traffic that is destined to FortiGate, also travels through the FortiLink interface.

You can create multiple FortiLink interfaces on a FortiGate to manage multiple FortiSwitch stacks. You can create the FortiLink interfaces in the same VDOM or different VDOMs.

You can manage FortiSwitch devices on FortiGate configured in standalone or HA mode. Both HA modes, active-passive (A-P) and active-active (A-A), support switch management. However, the VDOM where you configure the FortiLink interface must be operating in NAT mode. You cannot manage FortiSwitch devices on a transparent VDOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



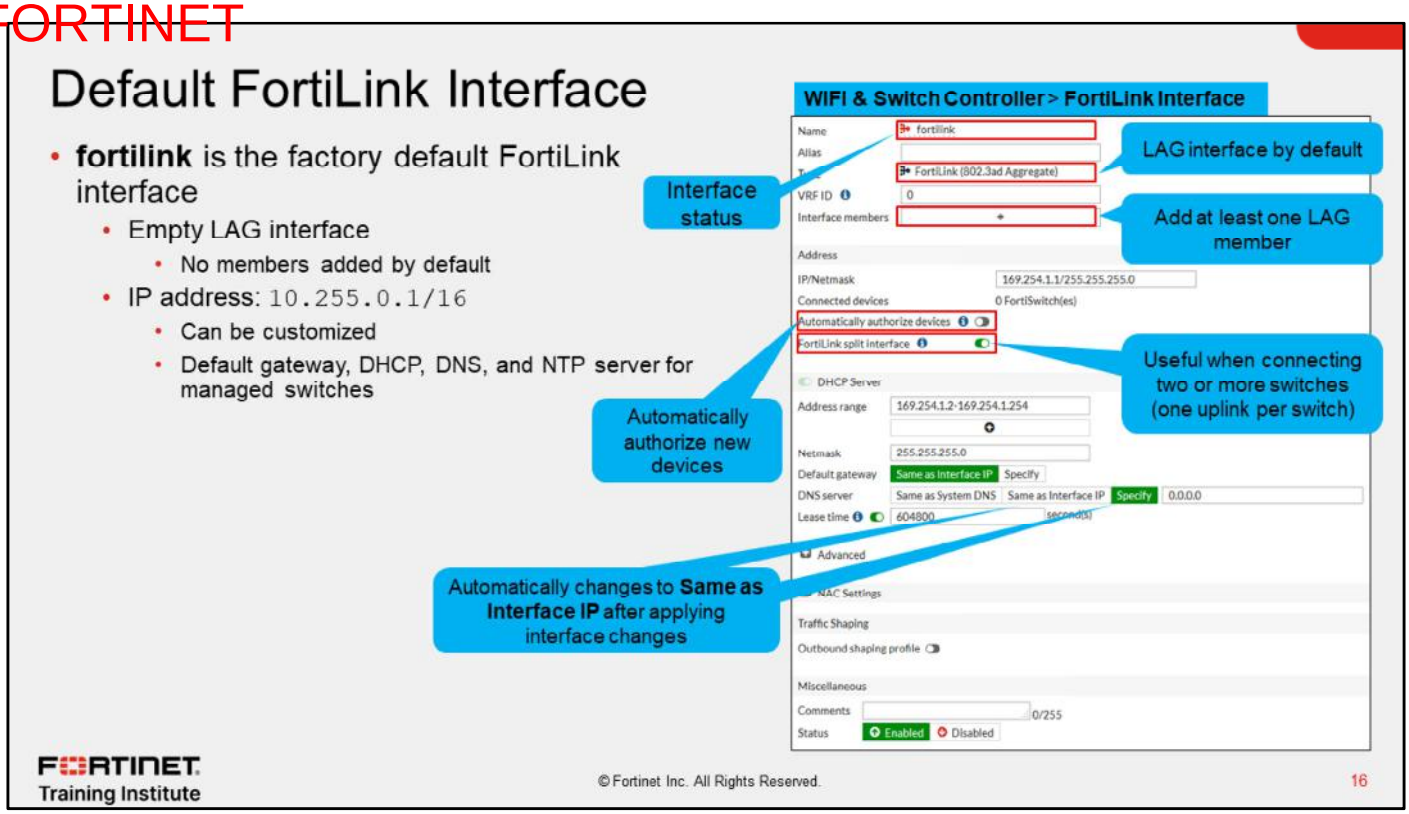
Regardless of the network topology you choose to deploy your managed FortiSwitch stack, the stack resembles a router-on-a-stick topology. The switch stack is connected to the FortiGate FortiLink interface, and therefore, all traffic between the stack and FortiGate is sent over this link.

From a logical perspective, the intra-VLAN traffic is handled by the switch stack. Because FortiGate is usually the default gateway for the endpoints connected to the switch stack, inter-VLAN traffic, internet traffic, and any other traffic that is protected by FortiGate, is sent to FortiGate through the FortiLink interface. FortiGate then processes the traffic based on the configured routing settings, firewall policies, and other related settings. For inter-VLAN traffic, FortiGate receives the user traffic tagged with the VLAN ID of the incoming VLAN interface, forwards the user traffic out of the outgoing VLAN interface, and tags it with the VLAN ID of the interface.

In addition, the switch management traffic is exchanged untagged and assigned to VLAN 4094 by default. VLAN 4094 is configured as the native VLAN on the FortiLink trunk, inter-switch links (ISLs), and inter-chassis links (ICLs). You will learn more about VLANs, FortiSwitch VLANs, ISLs, and ICLs in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



All FortiGate devices that support the switch controller feature come with a factory default FortiLink interface in the root VDOM named **fortilink**. The default FortiLink interface is a link aggregation group (LAG) interface with no LAG members by default. As a result, the administrator must add the LAG members manually. The interface is also assigned the `10.255.0.1/16` address by default. FortiGate uses the address and netmask to configure a DHCP scope for assigning addresses and other network parameters to managed switches.

In addition to acting as the default gateway and DHCP server for the managed switches, FortiGate also becomes their DNS and NTP server by default. Note that even though the default **DNS server** configuration under **DHCP Server** indicates **Specify**, the setting still automatically changes to **Same as Interface IP** after applying initial changes to the FortiLink interface.

By default, you must authorize the switches that FortiGate discovers before you can manage them. Alternatively, you can enable **Automatically authorize devices** to automatically authorize discovered switches. In addition, **FortiLink split interface** is enabled by default. When there is a FortiLink interface with two or more members, this option instructs FortiGate to keep only one FortiLink interface member active. This behavior is useful when you connect the FortiLink interface from one FortiGate device to two or more switches, and the switches do not support multi-chassis link aggregation (MCLAG) or MCLAG is not configured yet. In this scenario, you lose management to one or more switches if the FortiLink split interface is disabled. You will learn more about MCLAG and redundant network topologies in another lesson.

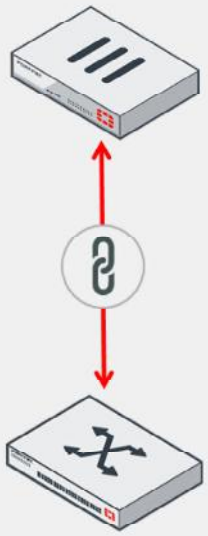
Finally, the GUI also displays a status icon. If the FortiLink interface is a LAG, then the icon indicates the status of the LAG.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Management Protocols

- FortiLink
  - Default FortiSwitch discovery method
    - In standalone, discovery frames are sent on specific ports
  - Also used for heartbeats
    - Between FortiGate and FortiSwitch only (FortiLink interface)
  - Discovery frames include switch serial number and port information
  - Ethernet type 0x88FF
- Link Layer Discovery Protocol (LLDP)
  - Alternative method for FortiSwitch discovery
  - Used for auto-ISL configuration (switch stack)
  - Ethernet type 0x88CC
- CAPWAP
  - Switch authentication and authorization
  - Also used for heartbeats
  - Alternative firmware upgrade method
  - LLDP neighbor information
  - FortiSwitch logs export
  - UDP port 5246



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

FortiGate uses multiple protocols to control FortiSwitch. The protocols listed on this slide are used mainly for switch discovery, authorization, and health checks.

For discovery, FortiGate uses the FortiLink protocol by default. The FortiLink discovery frames include the switch serial number, as well as the port information on the switch. Note that when FortiSwitch is in standalone mode, only specific ports send FortiLink discovery frames by default. For more information, refer to the *FortiSwitch—Managed by FortiOS* document on `docs.fortinet.com`. FortiLink is also used by managed switches that are directly connected to FortiGate to send heartbeats.

You can also use LLDP as an alternative switch discovery method. LLDP is also used when setting up a switch stack, because it enables the links connecting the switches to be automatically configured as trunks (auto-ISL). You will learn more about trunks and auto-ISL in another lesson.

CAPWAP is another control protocol that FortiGate uses to manage FortiSwitch devices. CAPWAP performs switch authentication, authorization, and health checks (heartbeats) by establishing a Datagram Transport Layer Security (DTLS) tunnel between FortiGate and the switch. It is also used as the alternative and legacy method for sending a firmware image file to a switch when you use the FortiGate GUI firmware upgrade tool. FortiSwitch also uses CAPWAP to send LLDP neighbor information and switch logs to FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Management Protocols (Contd)

- DHCP
  - Management IP address assignment
  - UDP port 67
- DNS
  - Name resolution
  - UDP port 53
- NTP
  - Time synchronization (critical for CAPWAP DTLS tunnel)
  - UDP port 123
- HTTPS
  - Configuration and diagnostics using REST API
  - Default firmware upgrade method
  - TCP port 443
- SSH
  - CLI connection tool on the GUI
  - TCP port 22



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

DHCP, DNS, NTP, and HTTPS are used for provisioning the switch with a management IP address, its time, name resolution, and configuration, respectively.

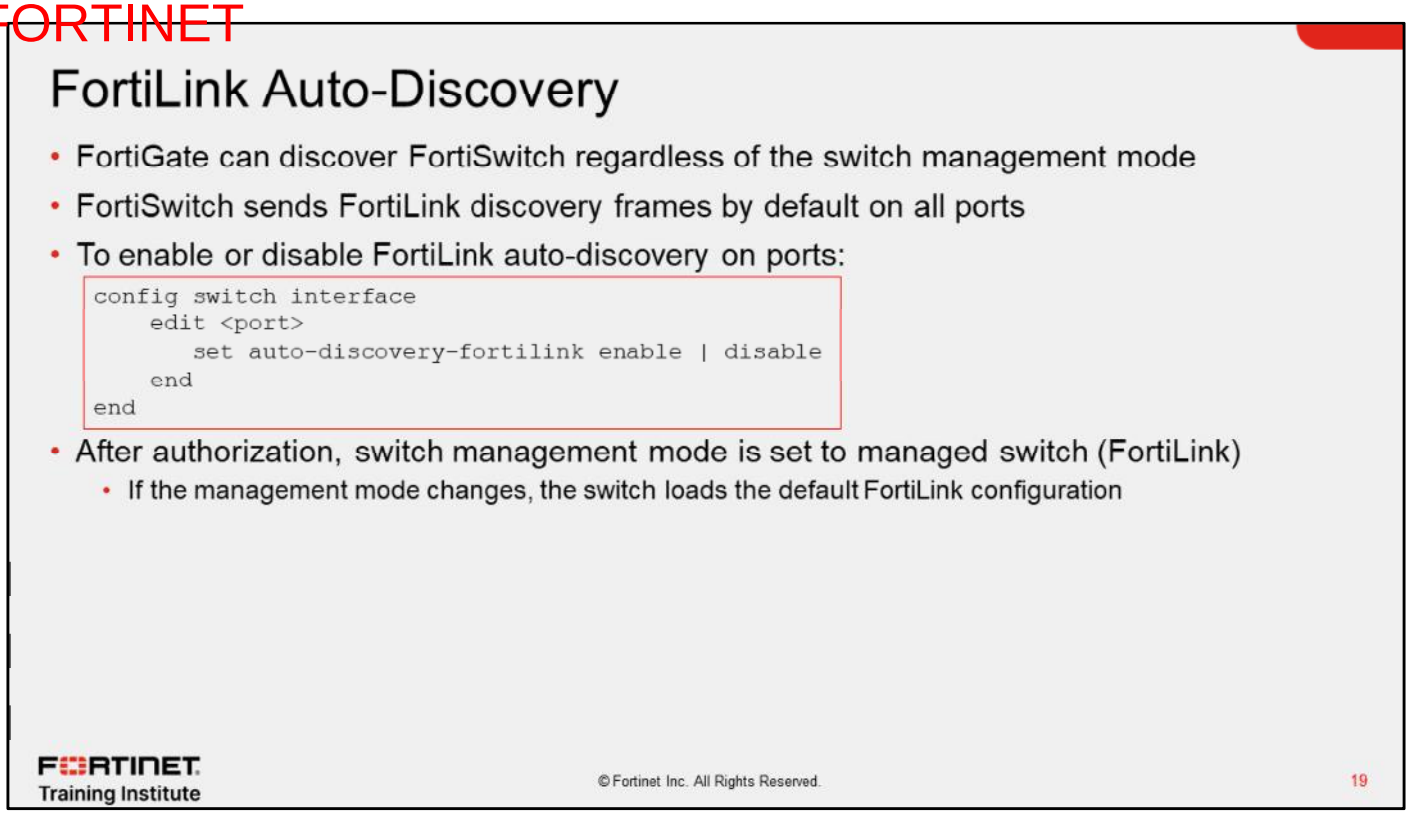
FortiGate acts as the DHCP, DNS, and NTP server for the switch. FortiSwitch uses DHCP to get an IP address from the same subnet as the FortiLink interface. In addition, FortiGate is configured to respond to DNS and NTP requests received at the FortiLink interface by default. The use of NTP is very important because the time on FortiGate and FortiSwitch *must be* in sync. Otherwise, the CAPWAP DTLS tunnel won't be established and therefore the switch won't come online.

FortiGate uses HTTPS for pushing switch configuration, collecting diagnostics, and as the switch default firmware upgrade method. For this, FortiGate uses the FortiSwitch REST API to communicate with the switch. For example, when you change the port configuration of a switch on FortiGate, FortiGate uses the FortiSwitch REST API to apply the changes on the switch. When you check the FortiSwitch ports on the GUI, FortiGate also uses the FortiSwitch REST API to obtain the current port status information from the switch. When you use the FortiSwitch firmware upgrade tool on the FortiGate GUI or CLI, FortiGate uploads the firmware image file to the switch through HTTPS.

Finally, FortiGate also uses SSH to access the switch CLI. When you use the CLI connection tool available on the GUI, FortiGate establishes an SSH connection to the switch management IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate can discover FortiSwitch, regardless of the FortiSwitch management mode.

Every FortiSwitch broadcasts FortiLink discovery frames on all ports, by default. FortiLink discovery frames contain information about the switch that FortiGate uses to create the switch configuration on the firewall. FortiGate discovers the switch after it receives FortiLink discovery frames from the switch. At this point, if they want to, the administrator can authorize the switch for management purposes.

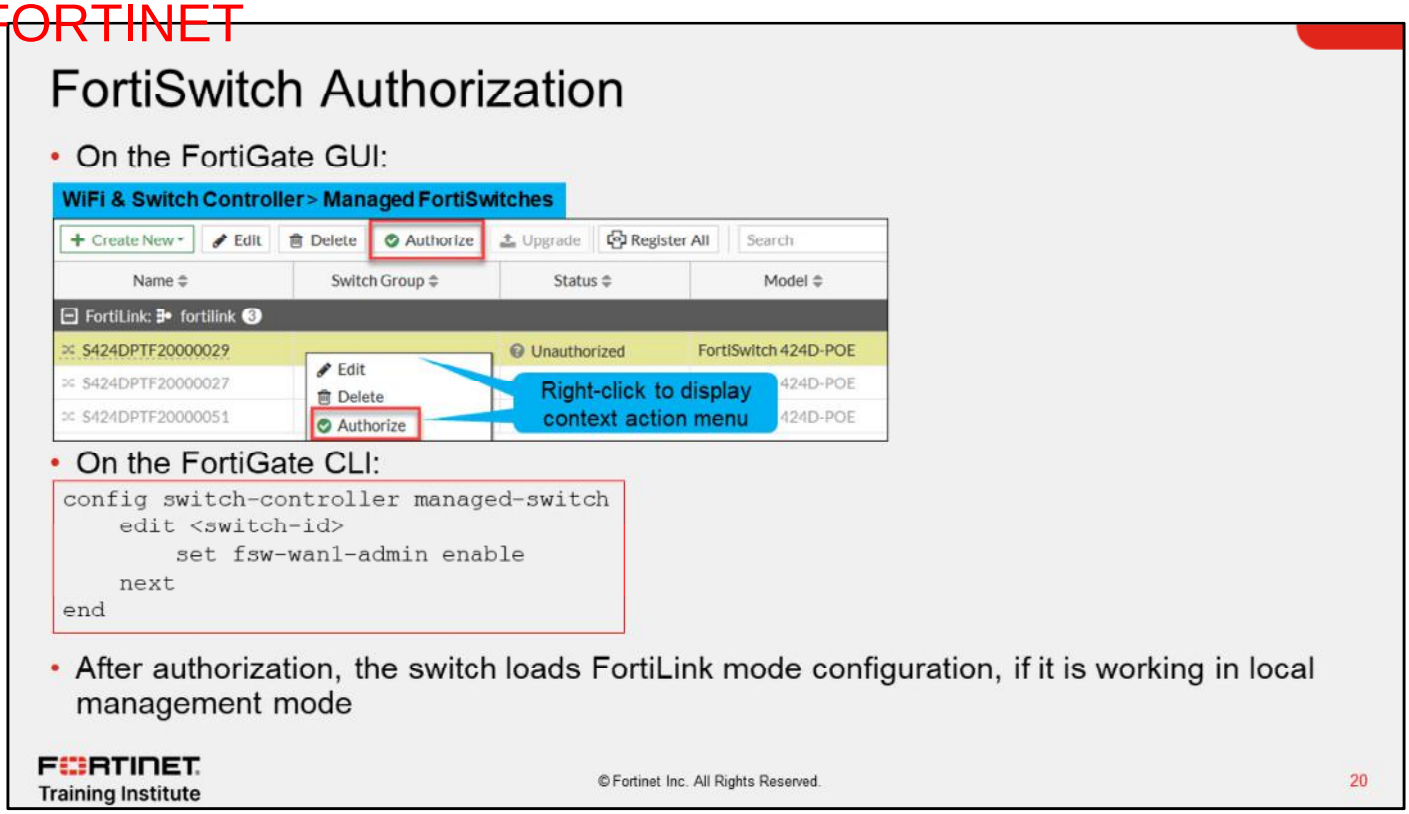
If you wish to disable auto-discovery on one or more ports, you can log in to the switch, and then disable `auto-discovery-fortilink` on the port so FortiGate cannot discover the switch through that interface.

When you authorize a switch that is working in standalone mode, the switch management mode is changed to managed switch mode (FortiLink mode). When FortiSwitch changes to managed mode, it is running the default FortiLink configuration. As a result, the configuration that the switch was running in standalone mode is lost.

Also, auto-network enables auto-ISL on all ports. For this reason, FortiSwitch automatically creates a trunk that has, as members, the ports that connect to the FortiLink interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If **Automatically authorize devices** is disabled on the FortiLink interface, you must manually authorize a switch on the FortiGate GUI or CLI before you can manage it.

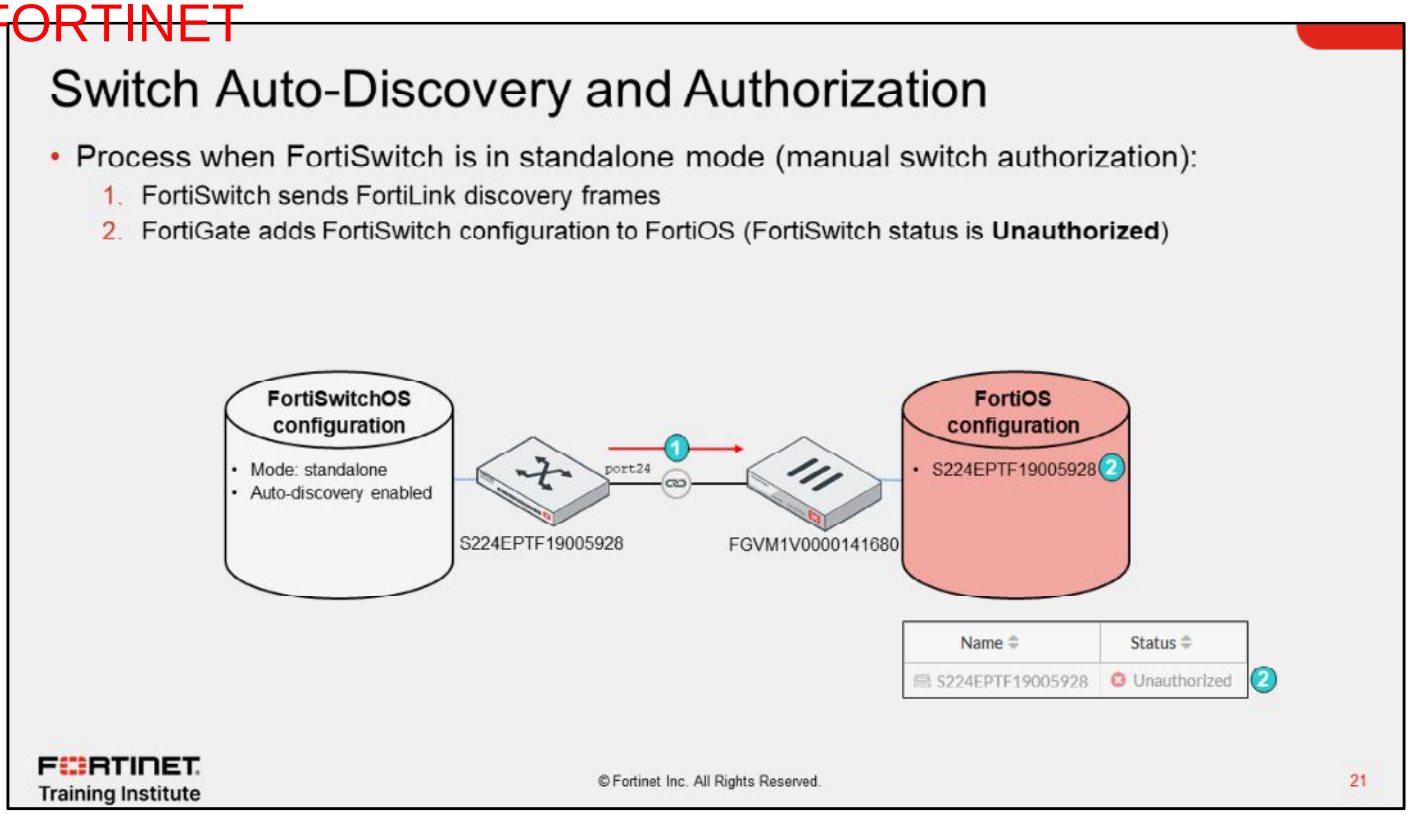
To authorize a switch on the FortiGate GUI, click **WiFi & Switch Controller** > **Managed FortiSwitches**, select the switch you want to authorize, and then click **Authorize** on the toolbar. Alternatively, you can right-click the switch to display a context menu, and then click **Authorize**.

You can also use the FortiGate CLI to authorize a switch by enabling the `fsw-wan1-admin` setting under the managed switch configuration, as shown on the slide.

Note that when you authorize a switch, FortiGate instructs the switch to set the management mode to FortiLink mode by sending a FortiLink frame to the switch. If, at this point, the switch is operating in local mode, FortiSwitch automatically changes the management mode to FortiLink mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide describes the switch auto-discovery and authorization process when you connect FortiSwitch in standalone mode to FortiGate. FortiGate has **Automatically authorize devices** disabled. In addition, the example on this slide indicates the serial number of each device, as well as the port used on FortiSwitch to connect to FortiGate. Based on the example, the process is as follows:

1. FortiSwitch sends FortiLink discovery frames to FortiGate. The frames are sent every 5 seconds and contain the switch serial number, model number, and firmware version.

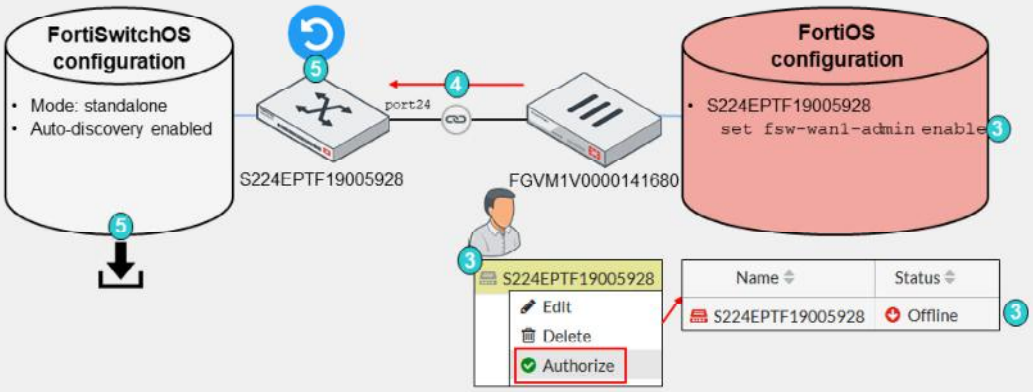
2. After receiving the FortiLink discovery frames, FortiGate adds the configuration of the newly discovered switch to FortiOS. The switch serial number, also known as the switch ID, appears in the list of managed switches as **Unauthorized**. The FortiSwitch port configuration added to FortiOS and the faceplate shown on the GUI for the switch, is based on the information contained in the FortiLink discovery frames. Also, if this is the first FortiSwitch that FortiGate discovers, FortiGate will also configure some additional settings required for FortiSwitch management, such as the default FortiSwitch VLANs, their DHCP scopes, and the quarantine replacement messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Switch Auto-Discovery and Authorization (Contd)

3. Administrator authorizes the switch on the FortiGate GUI (FortiSwitch status changes to **Offline**)
4. FortiGate sends a FortiLink frame to the switch to notify the authorization
5. FortiSwitch saves the standalone configuration and changes to default FortiLink configuration



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

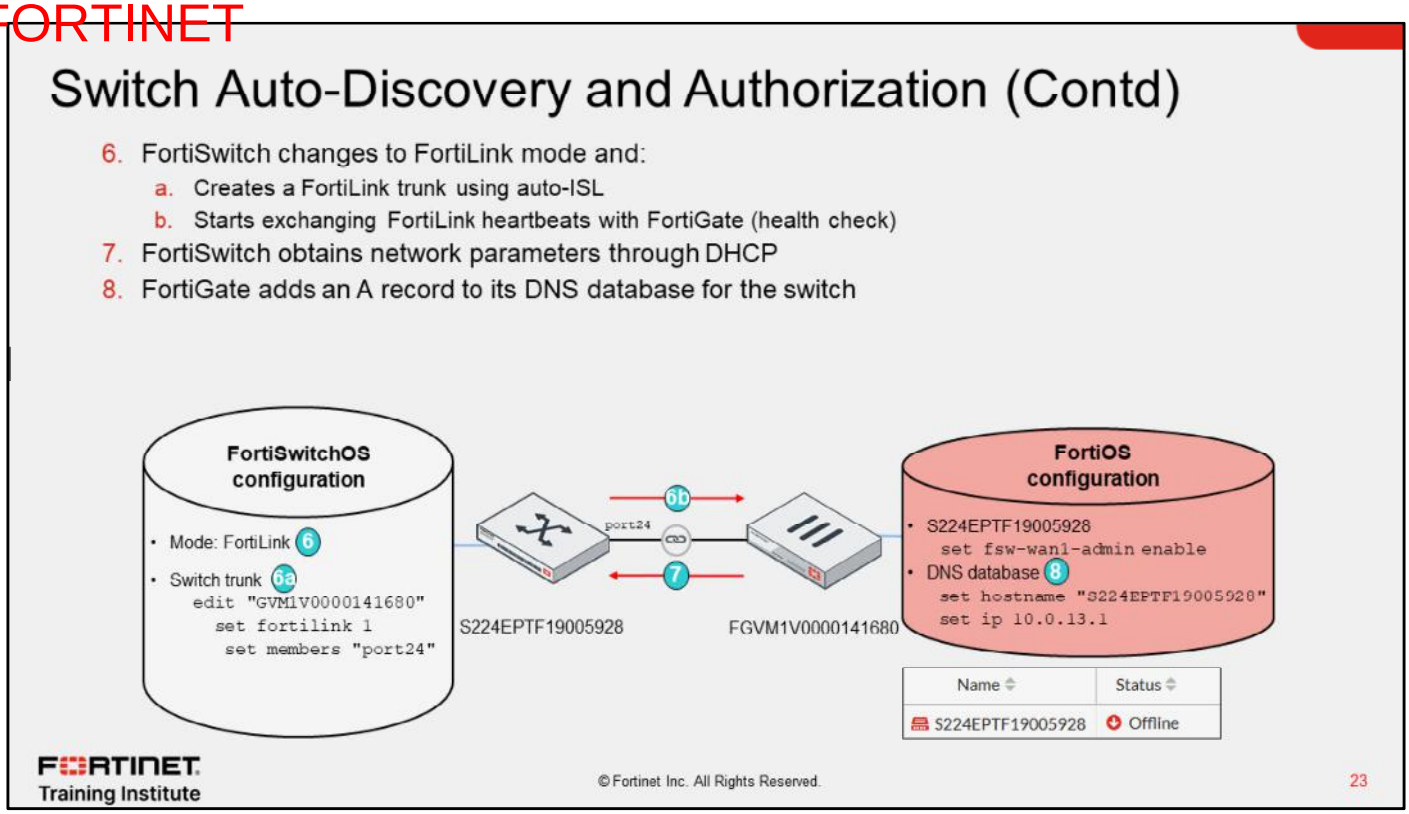
3. The administrator authorizes the switch on the FortiGate GUI, and as result, FortiOS enables the `fsw-wan1-admin` setting in the switch configuration. The FortiSwitch status also changes to **Offline**. The administrator can also authorize the switch on the FortiGate CLI by manually enabling the `fsw-wan1-admin` setting on the switch configuration, which is under `config switch-controller managed-switch`.

4. FortiGate sends a FortiLink frame to the switch to notify that it has been authorized.

5. FortiSwitch loads the default FortiLink configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



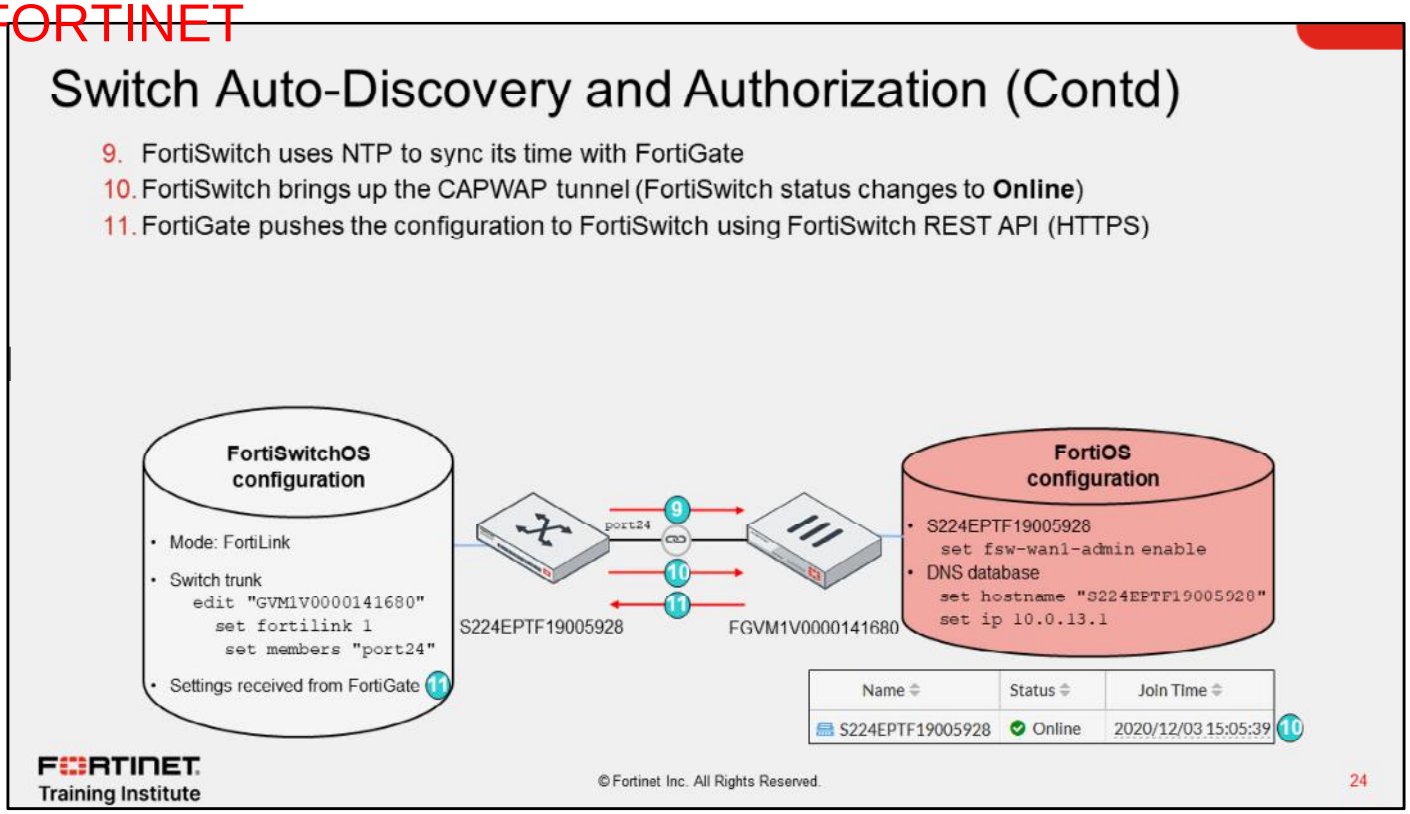
6. FortiSwitch changes to FortiLink mode and:
   a. Creates a FortiLink trunk using auto-ISL. The trunk contains the port connected to FortiGate as a member, and has the `fortilink` option set to `1`. The latter indicates that the FortiLink trunk was created on a switch that was detected using FortiLink as the discovery method.
   b. Starts exchanging FortiLink heartbeats with FortiGate for health checking purposes. Heartbeats are sent every three seconds.

7. FortiSwitch obtains its IP address and other network parameters from FortiGate through DHCP. The network parameters include FortiGate as NTP server, DNS server, and default gateway.

8. FortiGate adds an A record to its DNS database for the switch. The A record maps the switch serial number to its management IP address. In the example shown on this slide, the switch management IP address is `10.0.13.1`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



9. FortiSwitch uses NTP to synchronize its time with FortiGate. Time synchronization between FortiGate and FortiSwitch is key for the CAPWAP tunnel to come up. CAPWAP uses DTLS for data encryption. Because DTLS uses certificate-based authentication, a considerable time difference between the two devices will cause a DTLS handshake failure, and as a result, the CAPWAP tunnel will not come up.

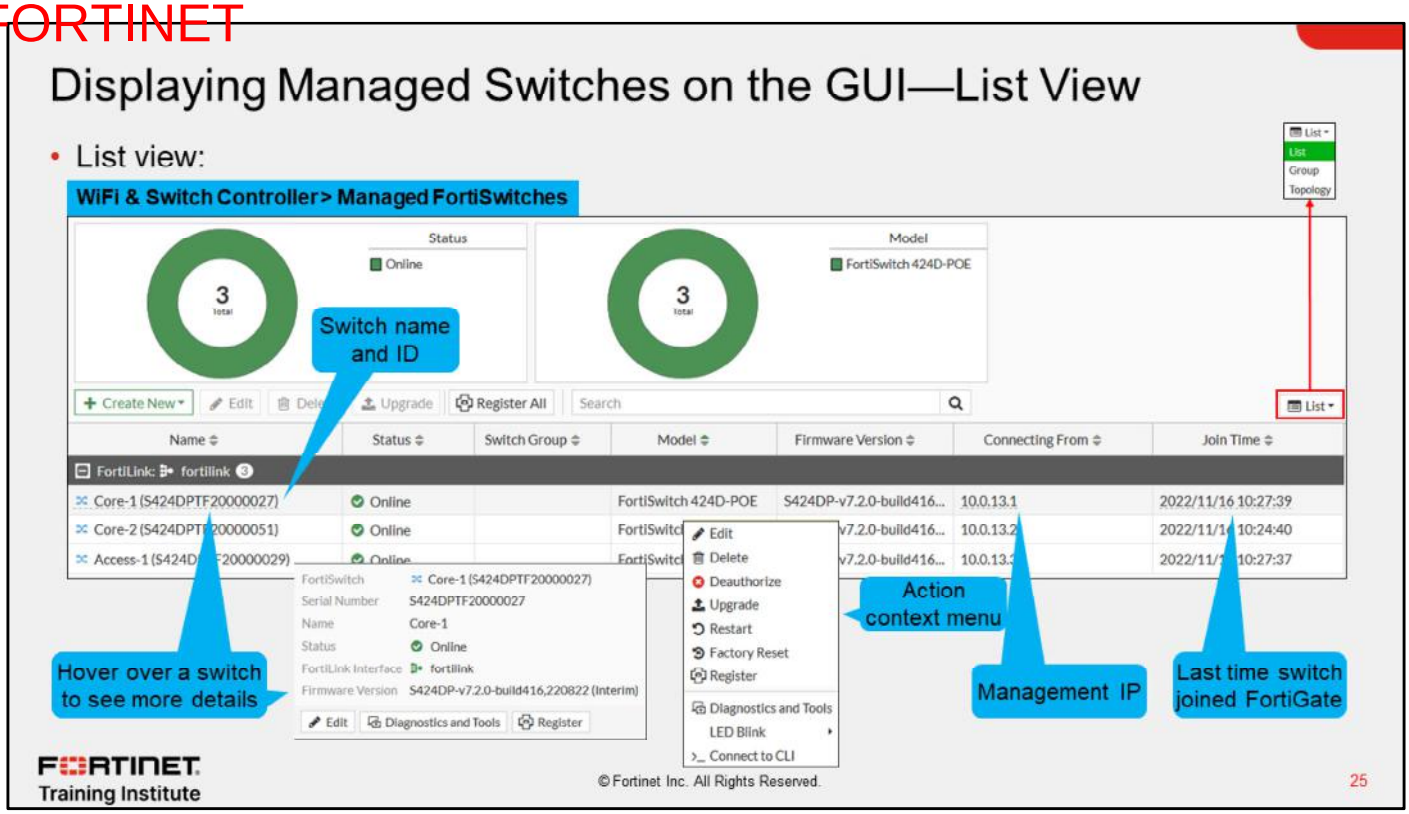
10. FortiSwitch brings up the CAPWAP tunnel. After the CAPWAP tunnel is established successfully, the FortiSwitch status changes to **Online**. The timestamp when FortiSwitch comes online is recorded as the **Join Time**.

11. FortiGate pushes the configuration to FortiSwitch using the FortiSwitch REST API. This connection is made over HTTPS.

At this point, the discovery and authorization process is complete. FortiGate and FortiSwitch continue exchanging data for health check, diagnostics, and configuration synchronization purposes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you authorize the switches, they eventually appear as **Online** on the **Managed FortiSwitches** page on the FortiGate GUI. By default, the page displays the switches in the **List** view, which is essentially a table that displays relevant information for each switch, such as the ID, status, management IP address, and join time.

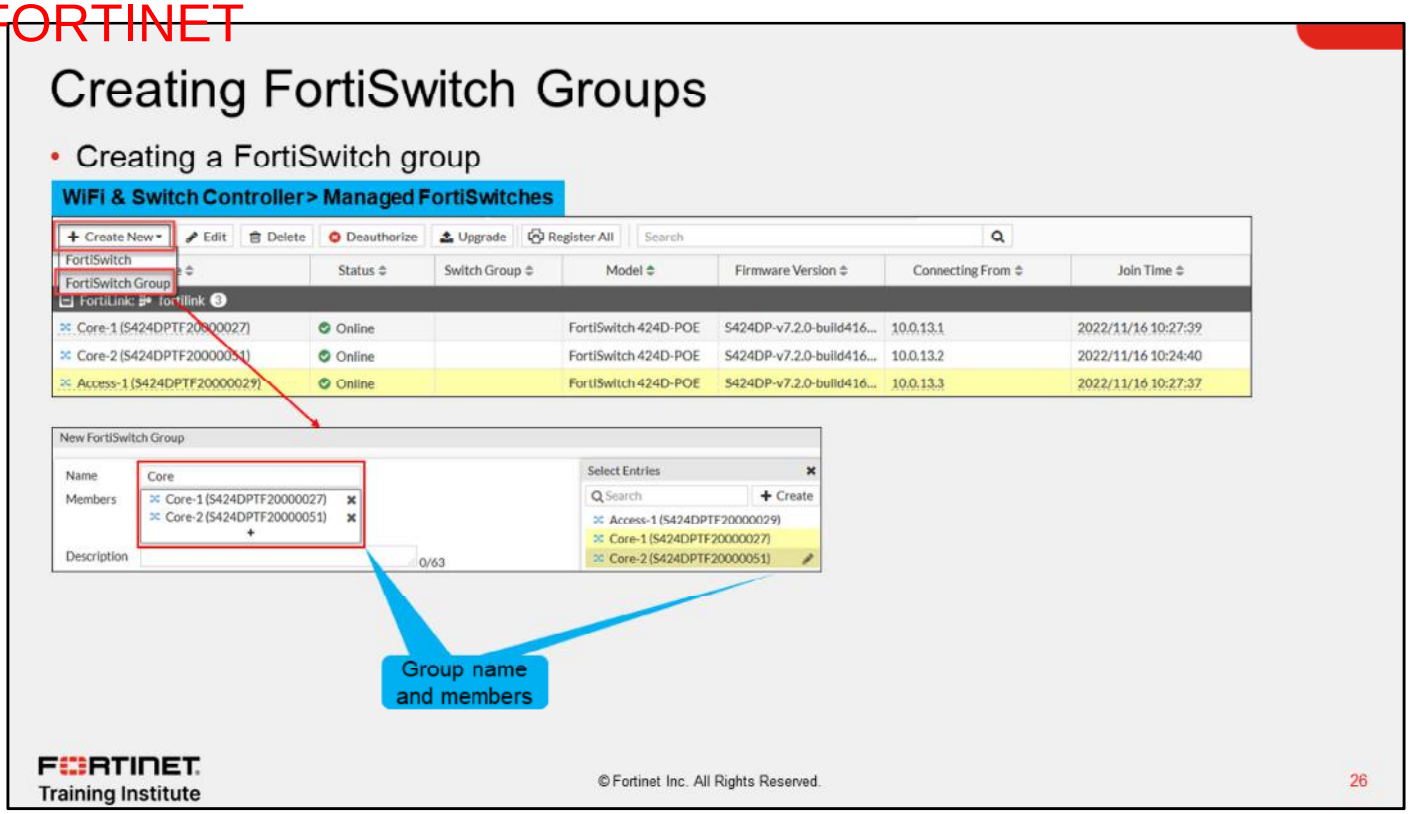
The join time, in particular, is a very important piece of information to look at. Under normal operation, a switch join time should remain the same. However, if a switch join time is frequently getting updated, this may be an indication of connectivity issues between the switch and FortiGate.

You can also hover over a switch to get more details, or right-click the device to display a context menu with some actions you can perform on the switch. The page also contains two pie charts that report on the switch status and models.

The **Managed FortiSwitches** page also offers two other view types: **Group** and **Topology**, which are described in the next slides.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

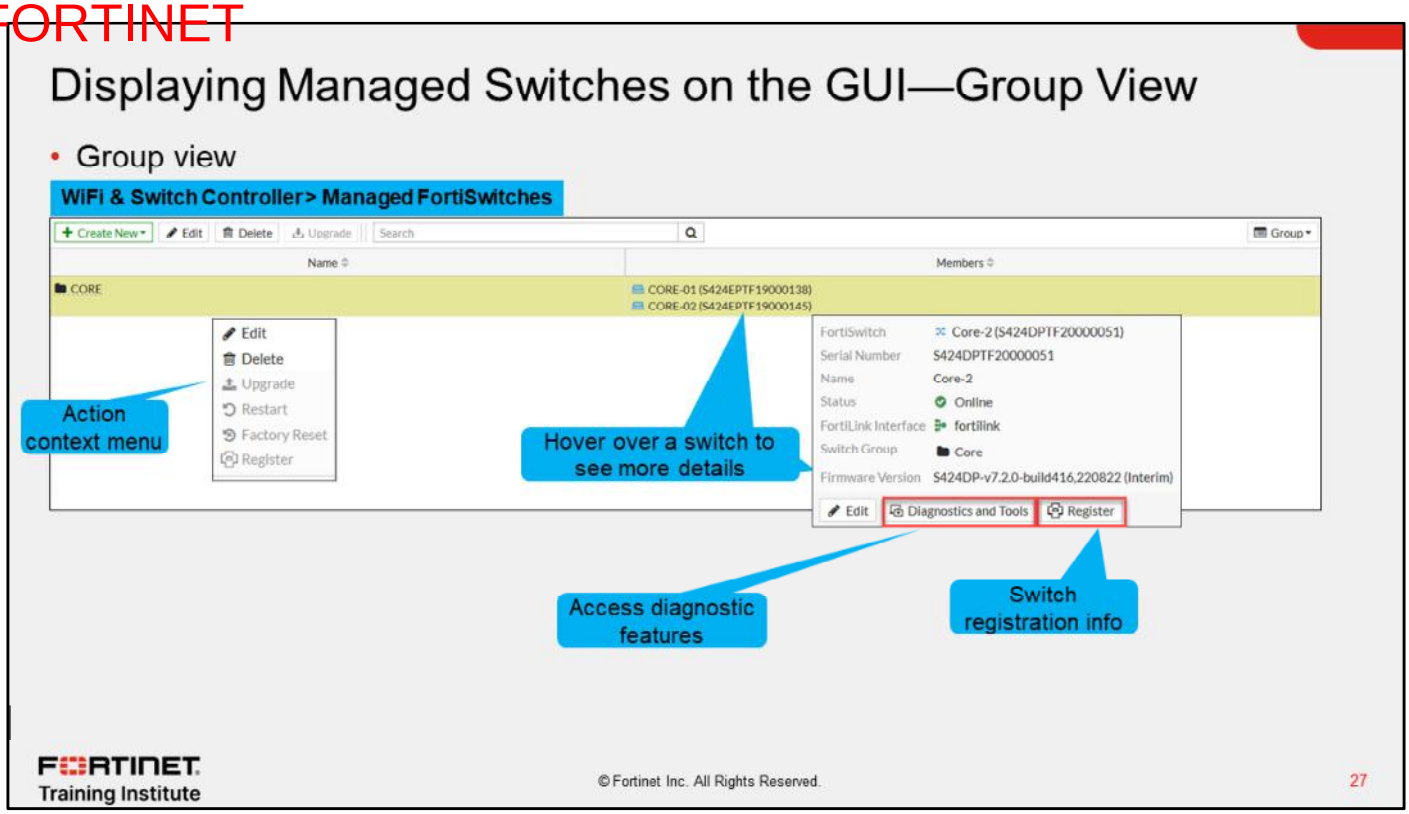


You can create FortiSwitch groups to speed up tasks that you need to perform on two or more devices. For example, you may want to restart a FortiSwitch group rather than restarting each individual switch, and therefore reduce administrative overhead. You may also want to perform a firmware upgrade on a group of devices instead of upgrading individual switches.

You create a FortiSwitch group on the **Managed FortiSwitches** page by clicking **Create New** > **FortiSwitch Group**. After you create the group, the GUI automatically changes to the **Group** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

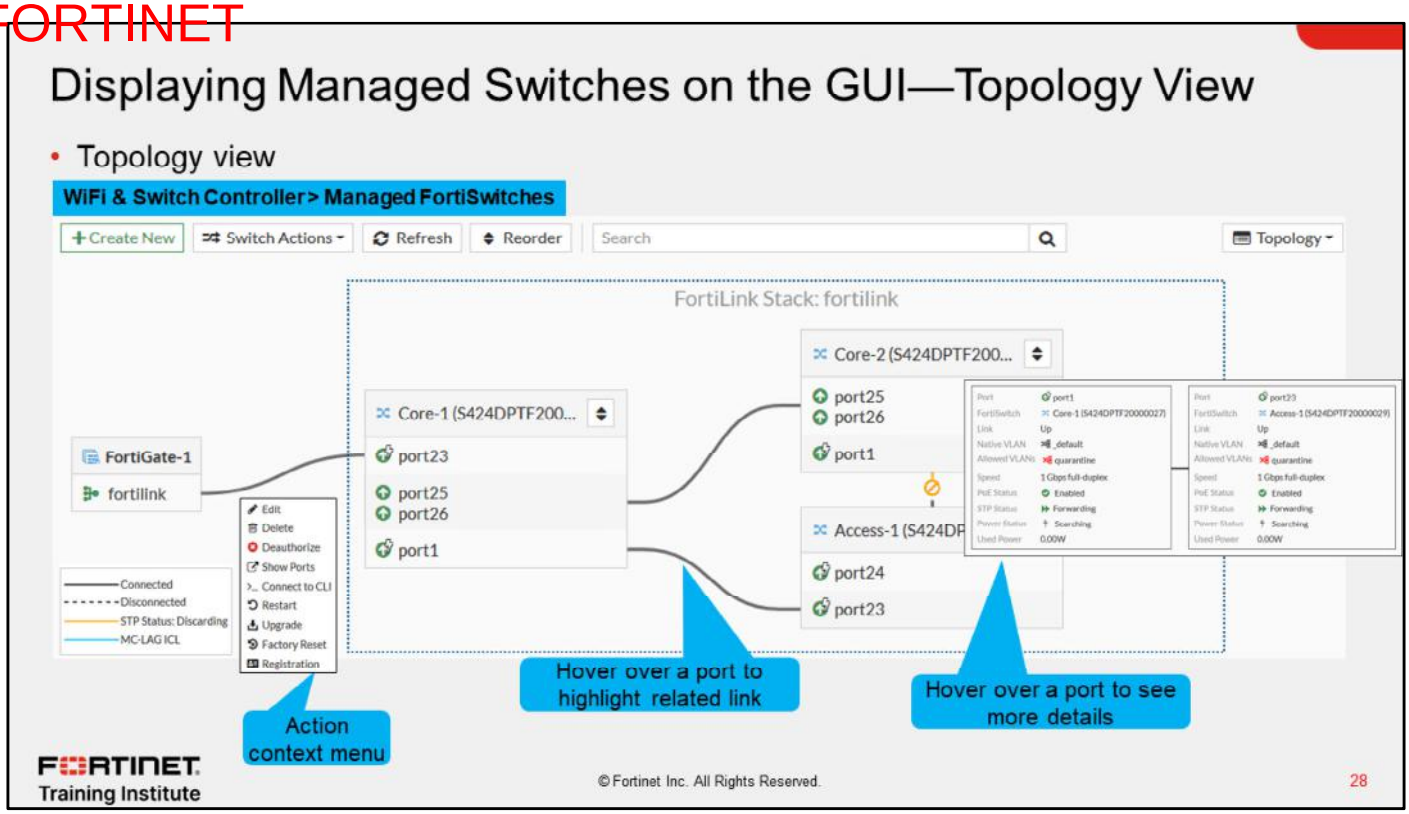


The **Group** view displays the configured FortiSwitch groups and members. Currently, there are a limited number of actions you can perform on a FortiSwitch group using the FortiGate GUI. For example, you can click **Register** on the context action menu to see the registration details for all devices in a group.

However, on the FortiGate CLI, there are more commands that you can use to perform an action on a specific FortiSwitch group.

Vouchers & Dumps are Available | WhatsApp +201224560923

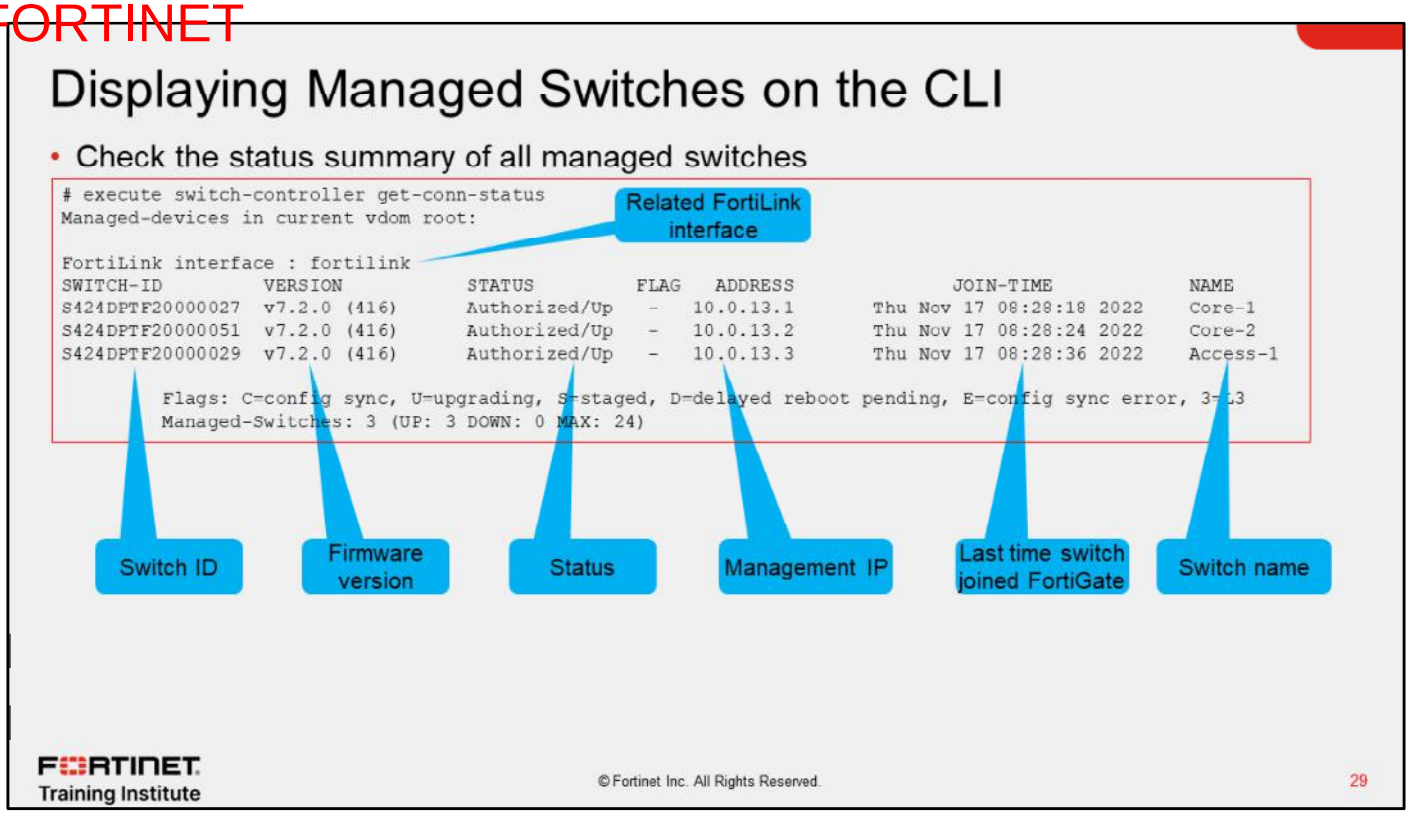
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Topology** view displays a simple but useful topology describing the physical links between switches, as well as the type of links. You can also hover over a port to see more details about the port, such as its status, native and allowed VLANs, operating speed, and STP state. You can also right-click a switch to display a context menu from where you can select an action, such as editing the switch settings, connecting to the switch CLI, factory resetting the switch, or upgrading the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



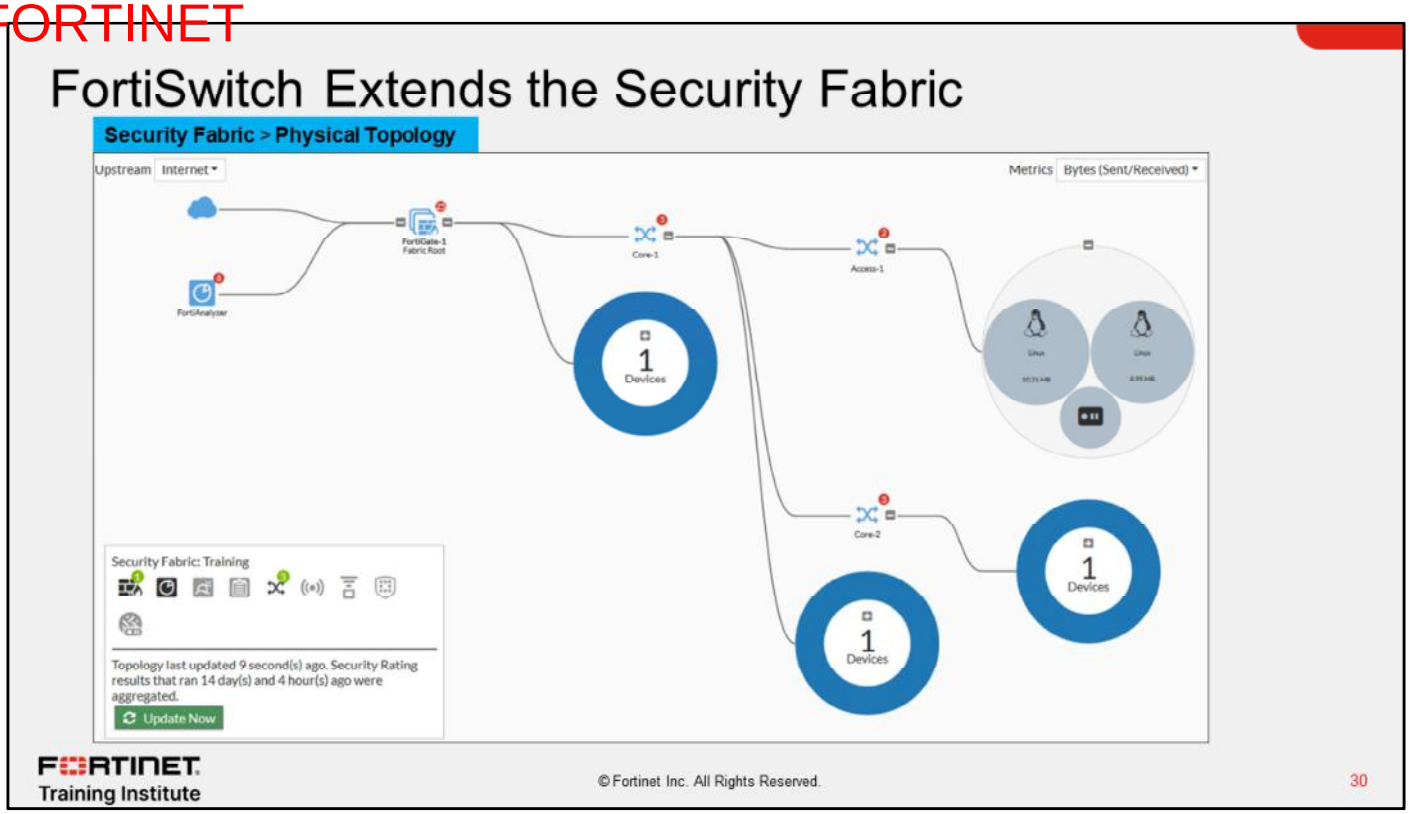
You can also display a list of managed switches using the FortiGate CLI. This slide shows the command you can run to get this information.

This command provides you with similar information as the list view on the **Managed FortiSwitches** page, except that it incudes a `FLAG` column which reports on the device operation status.

When you troubleshoot issues on a managed FortiSwitch stack, you likely start by running the CLI command shown on this slide, because it provides you with an overall status of the switches, including two pieces of information that you will likely need to troubleshoot further: the name of the FortiLink interface the stack is connected to and the ID of the switches in the stack. Because FortiGate supports the management of multiple switch stacks, and given that each stack can have multiple switches, knowing the FortiLink interface that the stack is connected to and the switch ID of a problematic switch will enable you to filter the output obtained when running troubleshooting commands. This is particularly useful when dealing with large FortiSwitch deployments, because going over the output of all managed switches can be overwhelming. In the example shown on this slide, the FortiLink interface is `fortilink`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



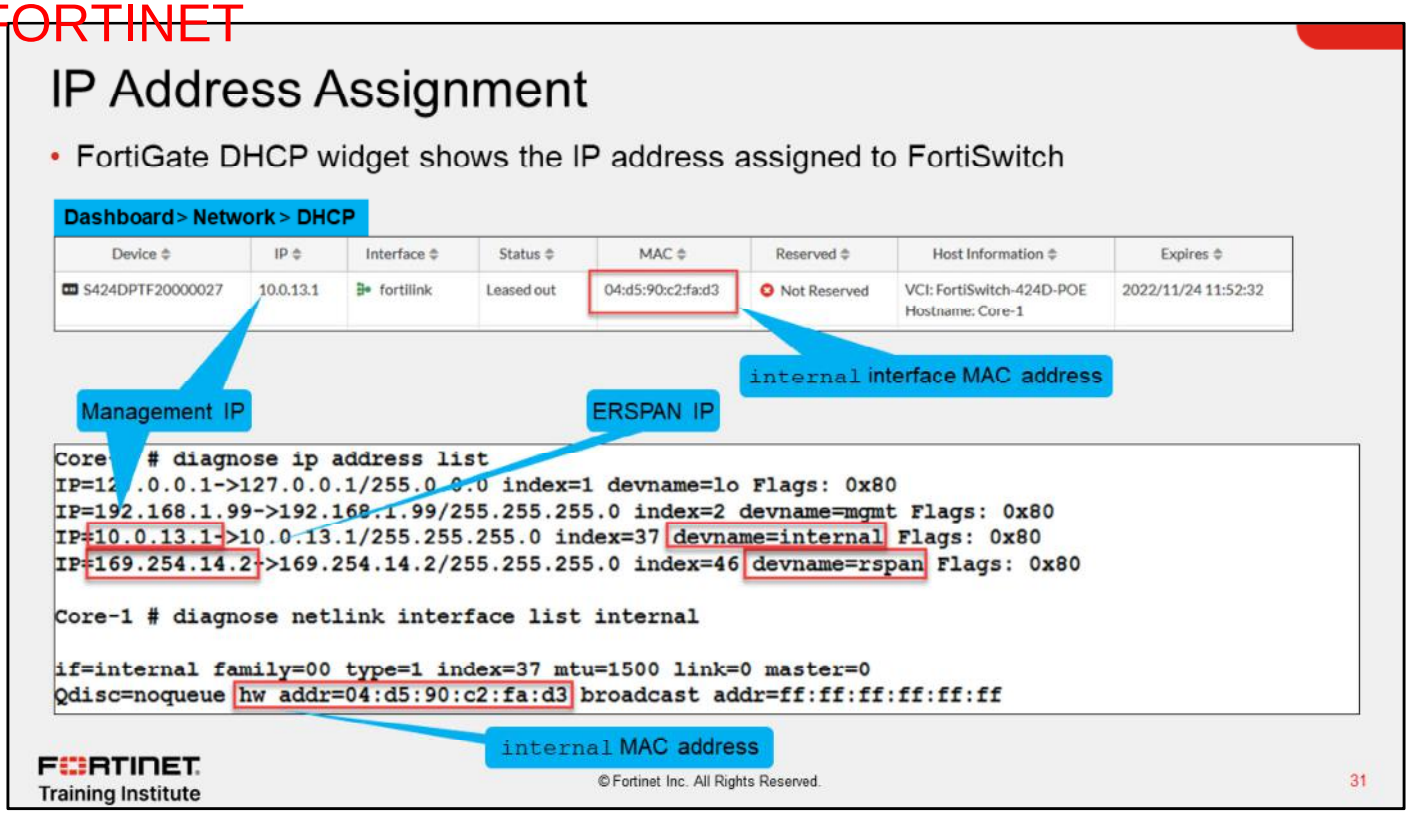
A managed FortiSwitch can be seen as an extension of FortiGate. In this way, FortiSwitch extends the visibility of the Fortinet Security Fabric up to Layer 2. Using FortiView physical and logical topology views, you can visualize different security segments together with all the stacked FortiSwitch and connected end devices.

In the example shown on this slide, the Security Fabric physical topology view shows a FortiGate controlling three FortiSwitch devices. The topology also displays the two Debian endpoints connected to the access switch.

Note that the physical topology does not show the full physical topology of the FortiSwitch stack. You can view the full physical topology in the **Topology View** on the **Managed FortiSwitches** page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After authorization, the switch requests two IP addresses from FortiGate through DHCP. On the FortiGate GUI, you can browse to the DHCP widget to display the IP addresses assigned to the managed switches. The IP addresses assigned to each switch over DHCP are:

- Management IP: The IP address is on the same subnet as the FortiLink interface. It is used for management communication between FortiGate and the switch. Although the slide does not show the FortiLink interface configuration, the interface has been assigned an address in the `10.0.13.0/24` subnet, which is why the assigned switch management IP is also in that subnet.

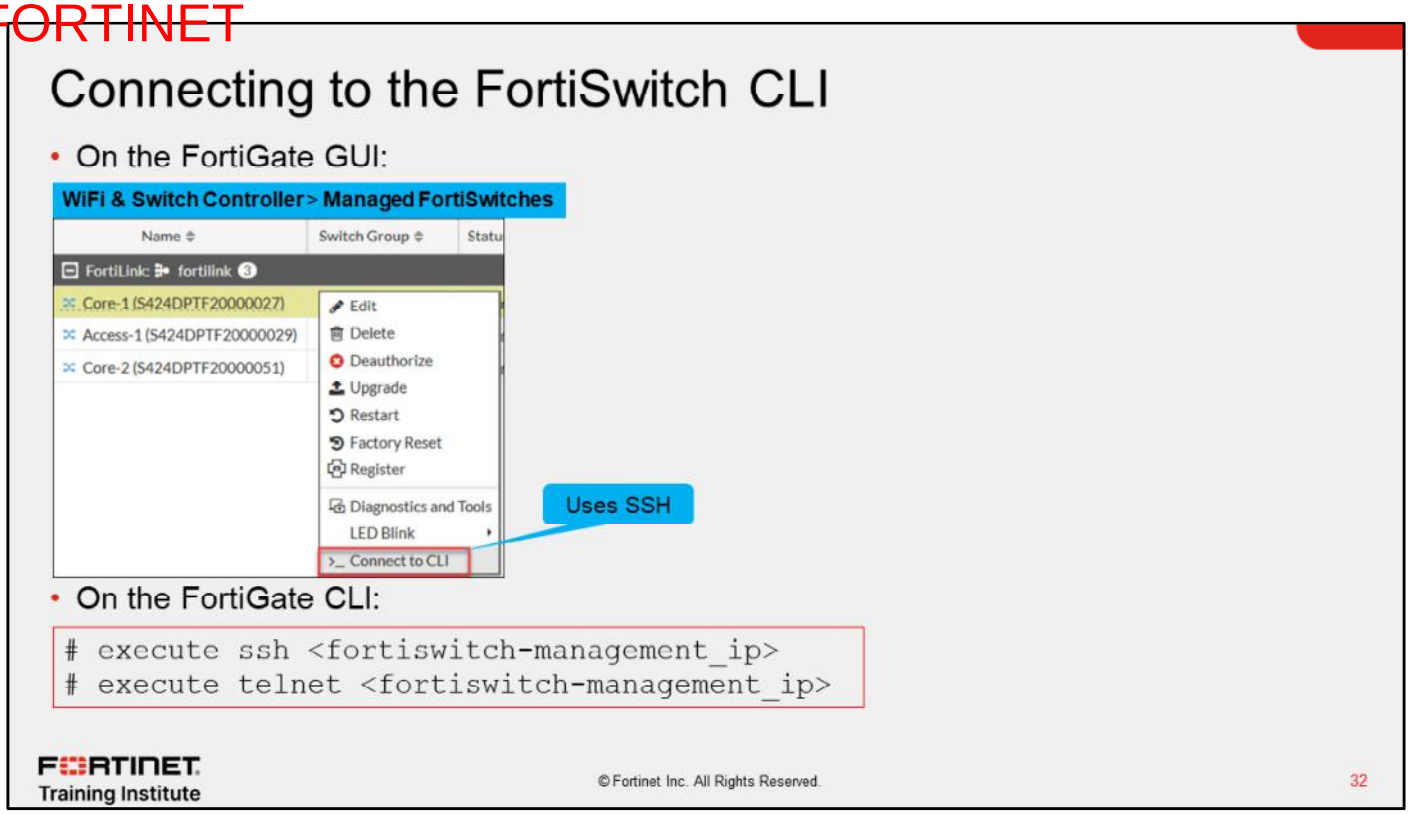
- ERSPAN IP: Encapsulated remote SPAN (ERSPAN) enables FortiSwitch to encapsulate mirrored traffic into GRE and send it across a Layer 3 network. The ERSPAN IP is used as the source IP address of the GRE packets. Note that although FortiSwitch also supports remote SPAN (RSPAN), this IP address is used by ERSPAN *only*. You will learn more about SPAN, RSPAN, and ERSPAN in another lesson.

The slide also shows the output of the FortiSwitchOS `diagnose ip address list` and `diagnose netlink interface list internal` CLI commands. The commands work in the same way as in FortiOS: they indicate the list of IP addresses assigned to the switch interfaces and some interface statistics, respectively. The output shows that the switch management and ERSPAN IPs are assigned to the `internal` and `rspan` interfaces, respectively. Because `rspan` is a VLAN interface bound to `internal`, both interfaces share the same MAC address.

The `internal` interface is a logical in-band management interface that is accessed through the switch ports. Some FortiSwitch models also come with a dedicated physical management port named `mgmt`, which provides you with out-of-band switch management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Once FortiSwitch is managed by FortiGate, you usually don't need to connect to the FortiSwitch GUI or CLI. All administration is done on FortiGate. However, if access to the FortiSwitch CLI is required, you can connect to it over SSH or telnet by running the commands shown on this slide. Just keep in mind that, by default, only SSH, HTTPS, and PING access are enabled on the switch `internal` interface. Therefore, if you want to connect to the FortiSwitch CLI over telnet, you must first enable telnet access on the switch.

You can also connect to the FortiSwitch CLI using the FortiGate GUI. When you use this method, FortiGate establishes an SSH connection to the switch management IP.

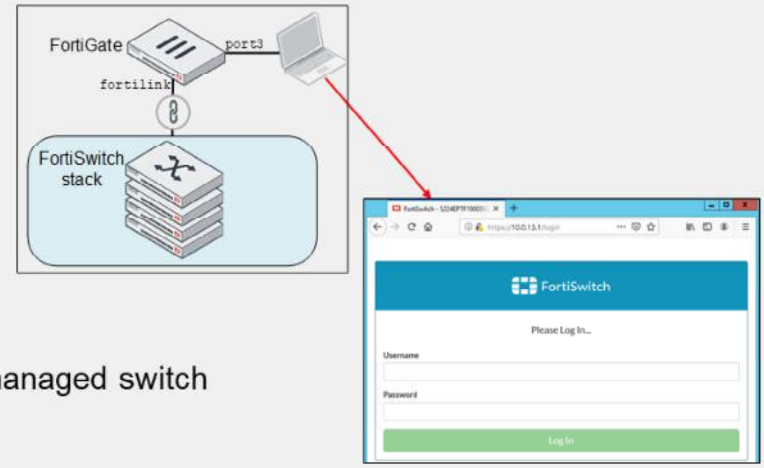
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Connecting to the FortiSwitch GUI

- Use a management workstation
  - Configure a firewall policy on the CLI to allow the connection, for example:

```
config firewall policy
    edit 1
        set name "toSwitches"
        set srcintf "port3"
        set dstintf "fortilink"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```



- Making changes directly on a managed switch is *not* recommended

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

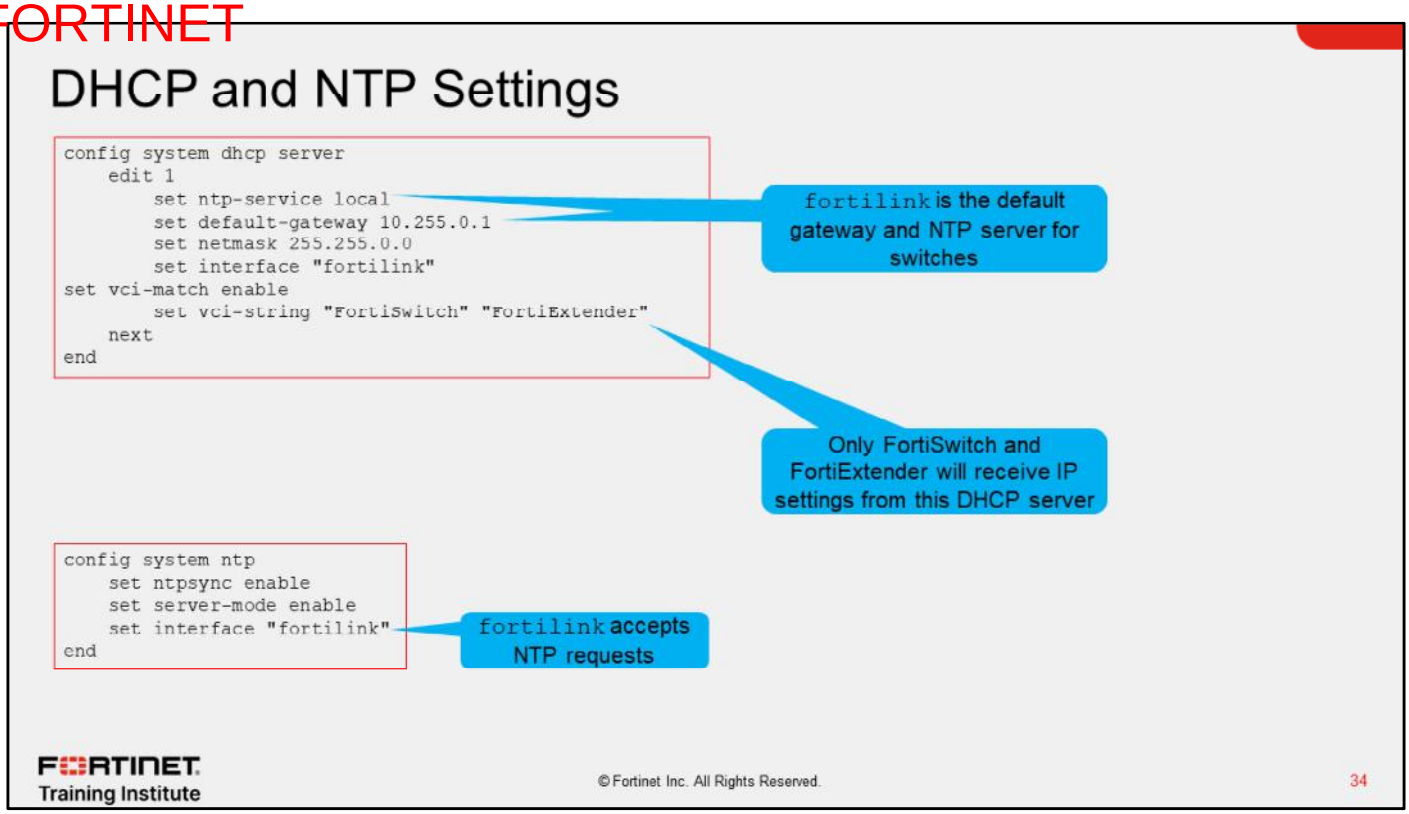
You rarely need to access the GUI of a managed switch. However, you can still access it by connecting to the switch from a management workstation in your network. By default, there are no firewall policies configured on FortiGate that allow traffic to the switch stack, so you must configure one for this purpose. Also, by design, the FortiGate GUI hides FortiLink interfaces from the list of available interfaces that you can reference in a firewall policy. This means that you must use the CLI to configure a firewall policy that allows traffic sourced from or destined to your switch stack.

This slide shows an example of a firewall policy configured on the CLI that allows traffic from a management workstation connected to `port3` on FortiGate to the default FortiLink interface. After you configure the firewall policy, you can access the FortiSwitch GUI by entering the switch management IP in the browser. Keep in mind that by default, FortiSwitch allows only HTTPS access to the GUI, and HTTPS redirection is not supported. This means that you must specify the HTTPS protocol when you enter the address in the browser, or if you want to use HTTP instead, you must manually allow HTTP access on the `internal` interface.

Note that making changes directly on the GUI or CLI of a managed switch is *not* recommended because the changes may be lost when FortiGate pushes a configuration to the switch when changes are made to the switch settings on FortiGate. For this reason, you should avoid making changes on the FortiSwitch directly, unless the setting is not available on the FortiGate, or when the switch operates in standalone mode. You will learn more about standalone mode and the FortiSwitch GUI in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

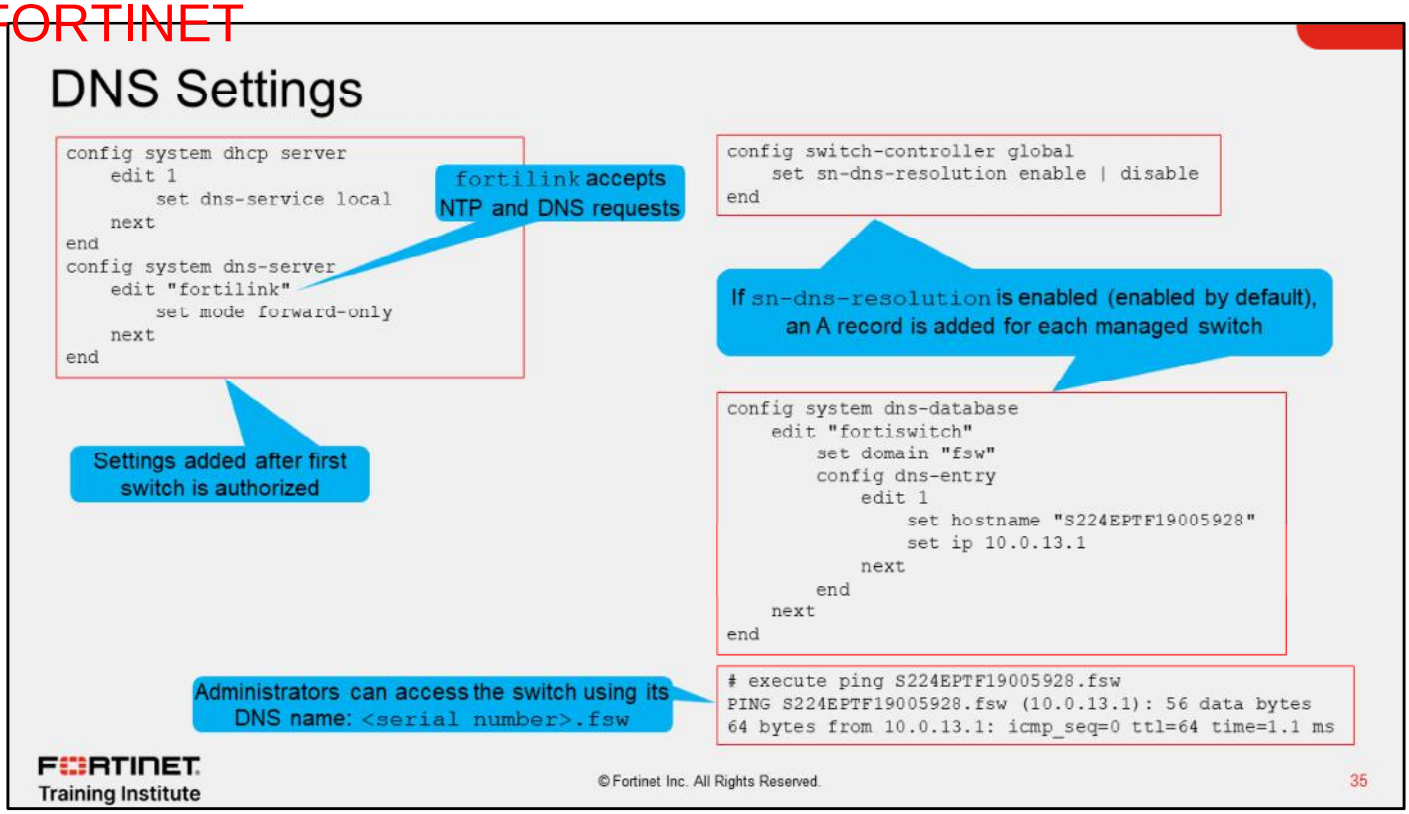


The default DHCP scope for the default FortiLink interface sets FortiGate as the default gateway, NTP server, and DNS server for its managed switches. The DHCP scope is automatically configured based on the IP address and netmask assigned to the interface. By default, the default FortiLink interface is assigned the IP address `10.255.0.1` and netmask `255.255.0.0`. In addition, the DHCP scope is also restricted to Vendor Class Identifiers (VCIs) `FortiSwitch` and `FortiExtender`. This means that only FortiSwitch and FortiExtender devices can obtain addresses from that scope.

For NTP, FortiGate is configured to respond to NTP requests received at the FortiLink interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

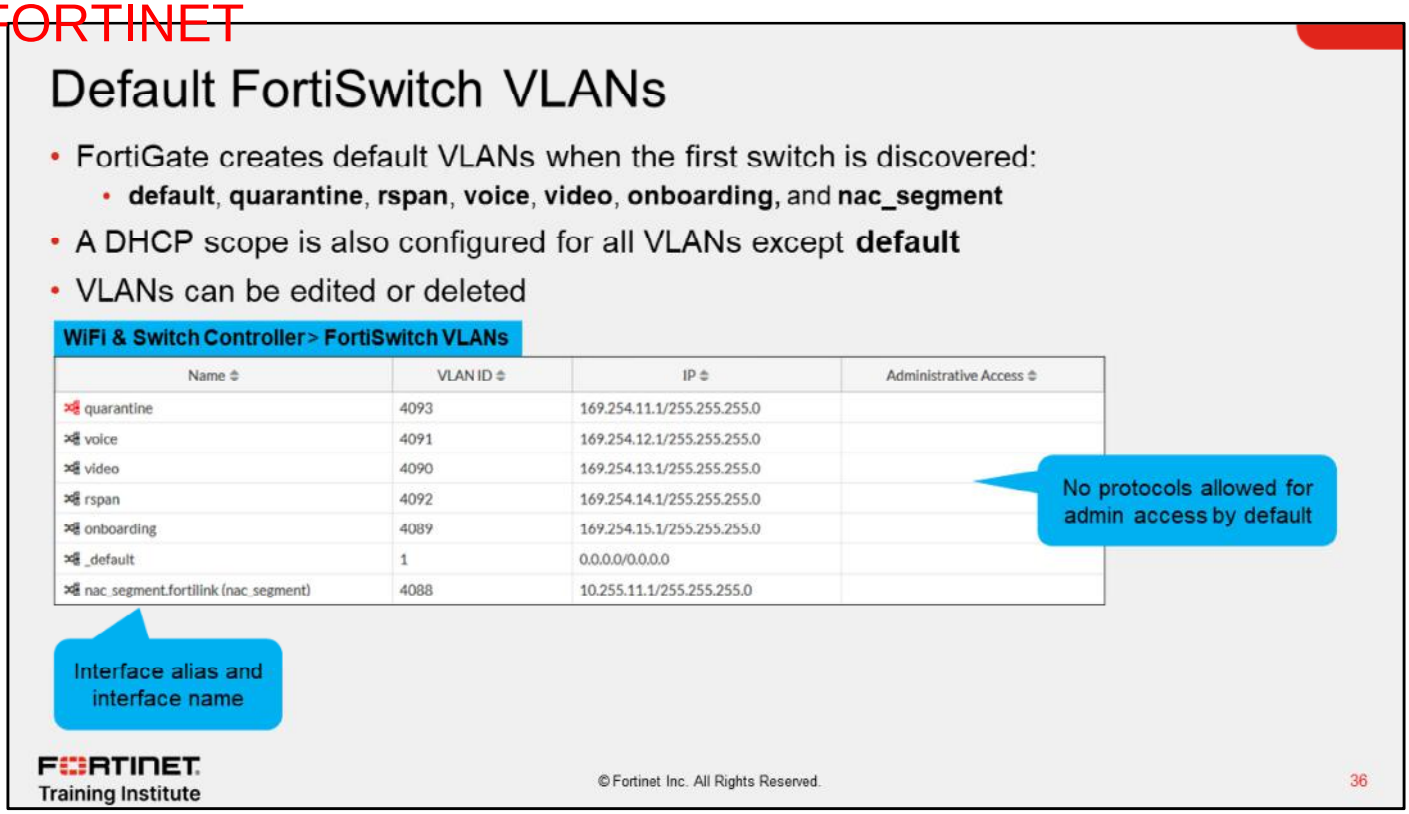


By default, FortiGate also acts as the DNS server for its managed switches. When you authorize the first FortiSwitch on FortiGate, FortiOS sets the `dns-service` setting to `local` in the DHCP scope configuration of the FortiLink interface, and adds the `fortilink` interface to the DNS server configuration so the interface can respond to incoming DNS queries made by switches.

In addition, after the switch obtains its management IP address from FortiGate, FortiOS also adds an A record that maps the switch serial number to the switch management IP. The result is that the administrator can ping or connect to the switch by using a DNS name that follows the syntax `<switch-id>.fsw`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When FortiGate discovers the first switch, FortiGate automatically adds some settings to its configuration that are required for switch management. These settings include the following FortiSwitch VLANs:

- **default**: This is the default native VLAN assigned to all switch ports.
- **quarantine**: This is the default VLAN used for quarantined traffic. On FortiGate, you can quarantine a device that is connected to a switch, and then the device is placed in the quarantine VLAN.
- **rspan**: This is used for sending encapsulated mirrored traffic across the network.
- **voice**: When using LLDP-Media Endpoint Discovery (LLDP-MED), you can assign the switch port to this VLAN, if the endpoint is detected as a voice device.
- **video**: This is the same as the voice VLAN, but is used when the endpoint is detected as a video device.
- **onboarding**: When network access control (NAC) policies are enabled, this is the VLAN where devices that do not match any of the configured NAC policies are placed. You will learn more about NAC policies in another lesson.
- **nac_segment**: This is used for NAC VLAN segmentation. You will learn more about NAC in another lesson.

In addition, a DHCP scope is configured for all VLANs except the **default** VLAN. Note that the DHCP configuration is not shown on this slide.

Finally, the VLANs are also assigned the predefined VLAN IDs shown on this slide and no admin access protocols, by default. You can edit or delete the default VLANs, if required. You will learn more about VLANs and FortiSwitch VLANs in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the default firmware upgrade method on a managed switch?
   A. CAPWAP
   ✓ B. HTTPS

2. What protocol does FortiGate use to inform FortiSwitch of its authorization?
   A. CAPWAP
   ✓ B. FortiLink

3. What FortiSwitchOS CLI setting controls the automatic broadcast of FortiLink discovery frames on a switch port?
   ✓ A. `auto-discovery-fortilink`
   B. `switch-mgmt-mode`

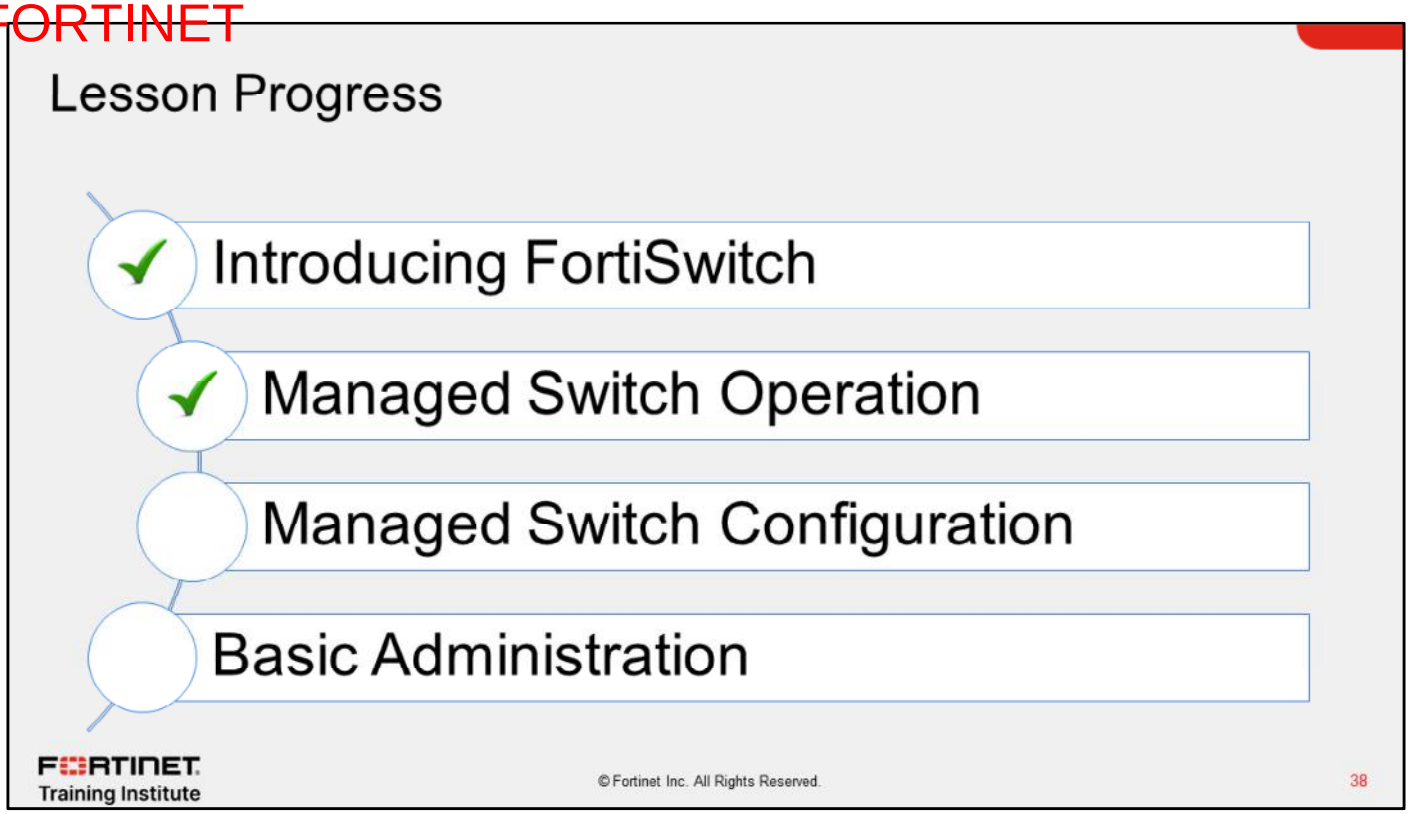
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

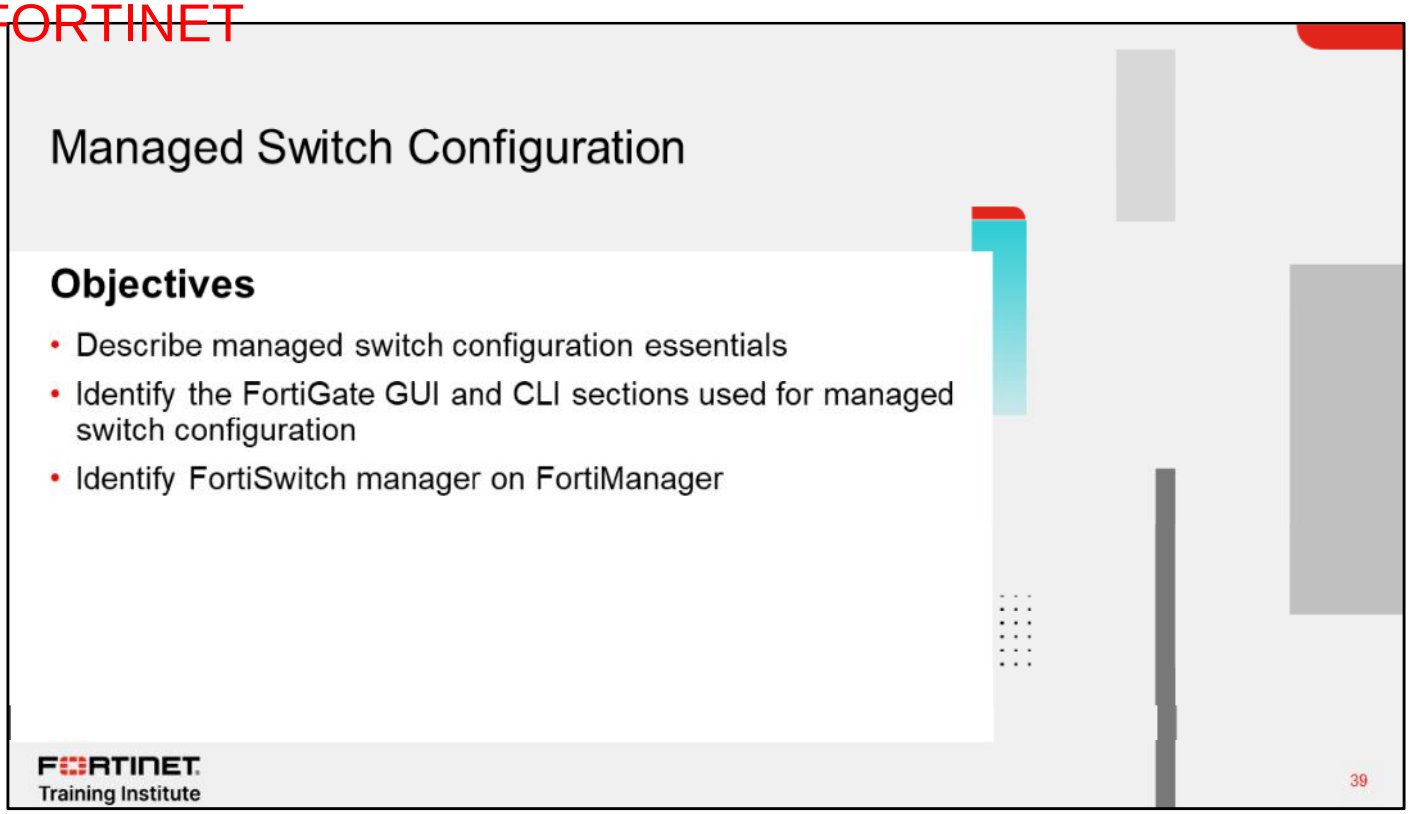


Good job! You now understand managed switch operation.

Now, you will learn about managed switch configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

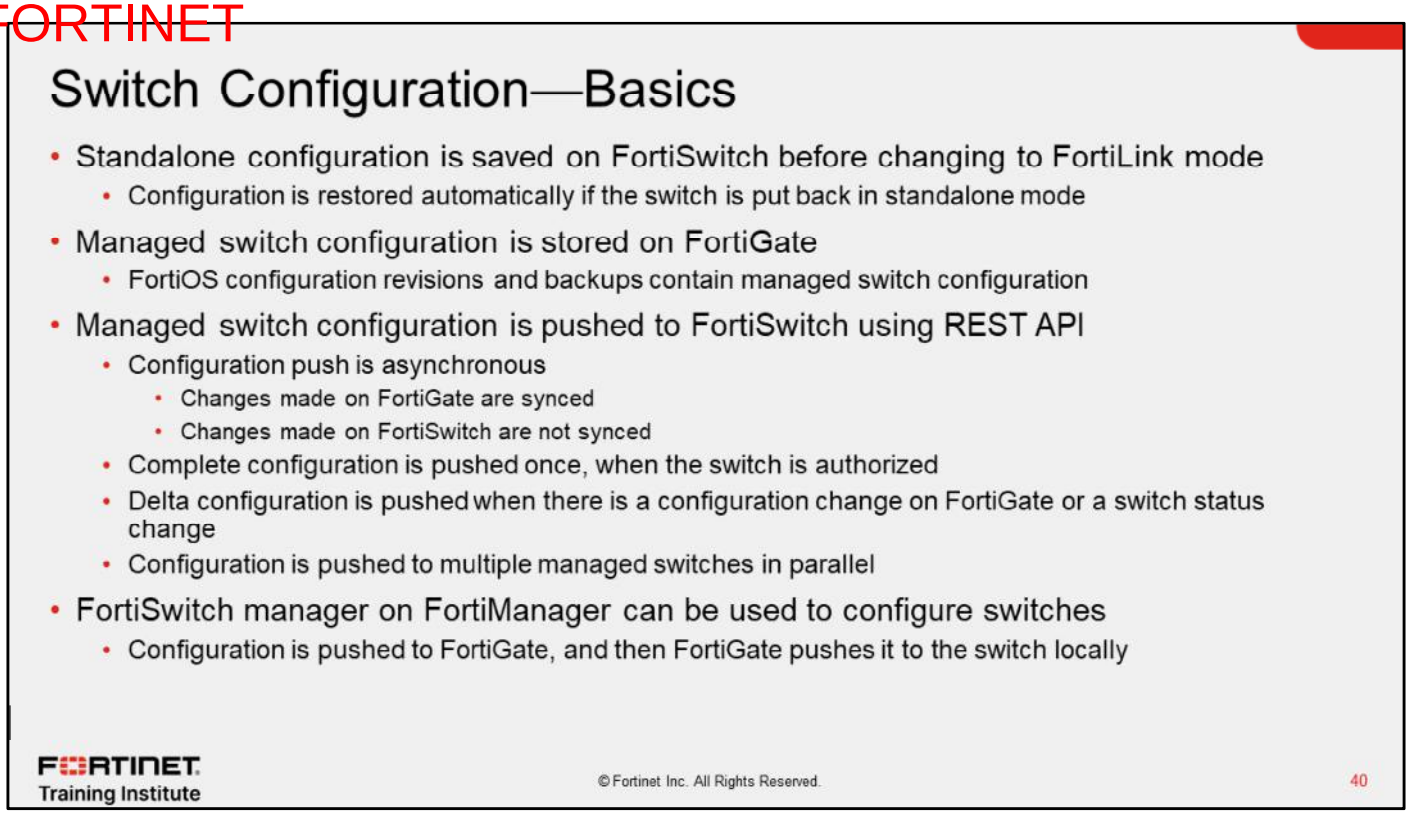


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managed switch configuration, you should be able to identify the configuration layout used by FortiGate and FortiManager for switch management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you authorize a switch that is working in standalone mode, the switch configuration is saved locally just before the switch changes to FortiLink mode. Later, if you change the management mode back to standalone, the switch automatically restores the configuration that was backed up previously.

The configuration for a managed switch is stored on FortiGate, and it's part of the FortiOS configuration file. For this reason, configuration revisions generated on FortiGate and configuration backups made by the administrator also contain the configuration for all managed switches.

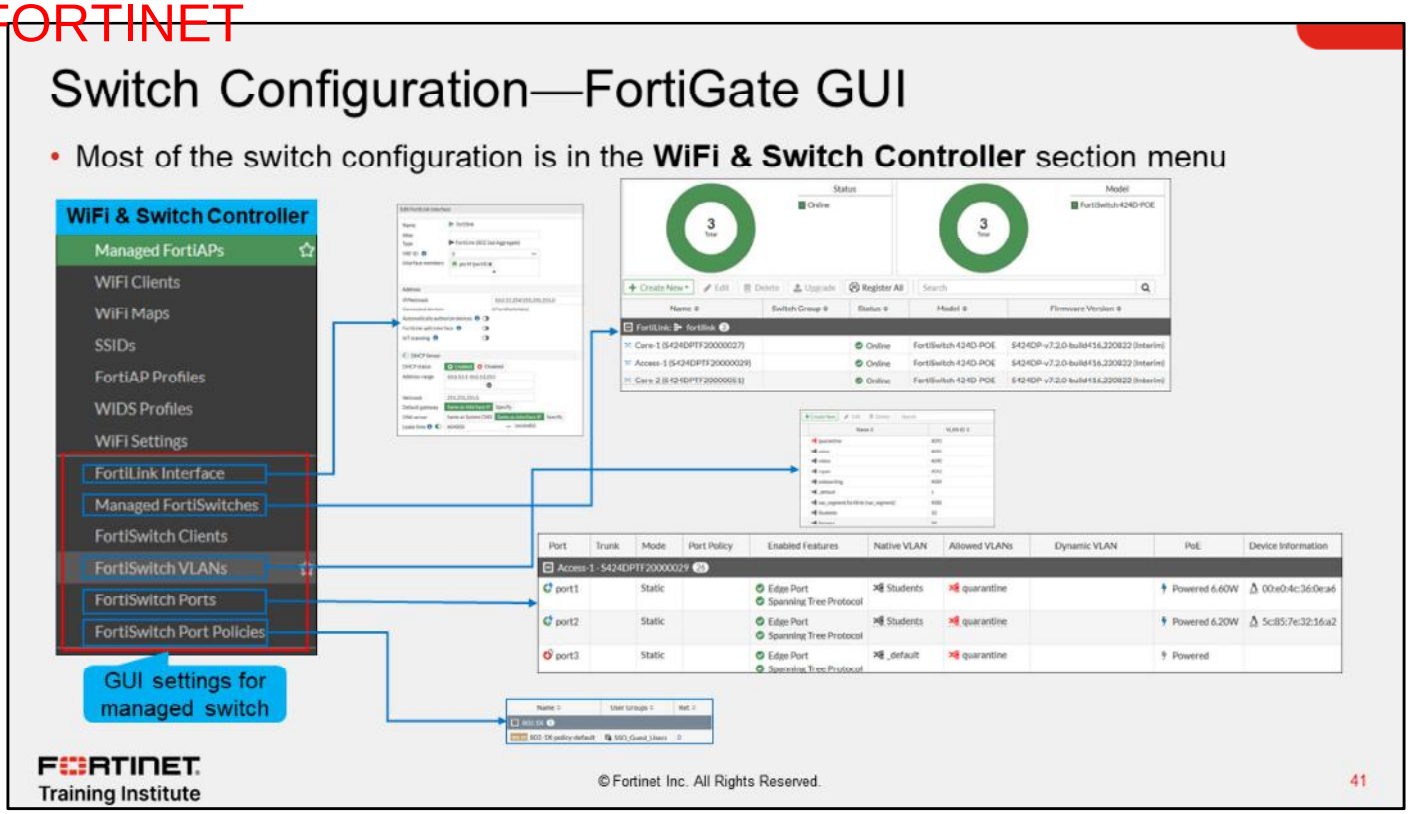
When you configure a managed switch on FortiGate, the configuration is pushed to the switch using the FortiSwitch REST API. The configuration push for a managed switch follows an asynchronous model. This means that only configuration changes made on FortiGate are pushed to the switch, while configuration changes made directly on the switch are not synced to FortiGate. As a result, configuration changes made directly on the switch may be lost, and therefore, not recommended.

To improve performance and scalability, FortiGate pushes the complete configuration for a switch only once, which is after switch authorization. After that, FortiGate pushes only the changes made by the administrator, also known as the delta configuration. Also, if the switch status changes from offline to online, FortiGate also pushes the delta configuration only, provided there were changes made to the switch while it was offline. The switch status can change between offline and online because of a reboot, firmware upgrade, or another type of network disconnection event. In addition, if you have multiple managed switches, FortiGate pushes the configuration to multiple switches at the same time.

Finally, if you manage FortiGate from FortiManager, by extension, you can also manage the FortiSwitch stack on FortiManager. For this, you use the FortiSwitch manager pane on FortiManager to edit the switch settings, and then you push the changes to FortiGate, which in turn, pushes them to the switch locally.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



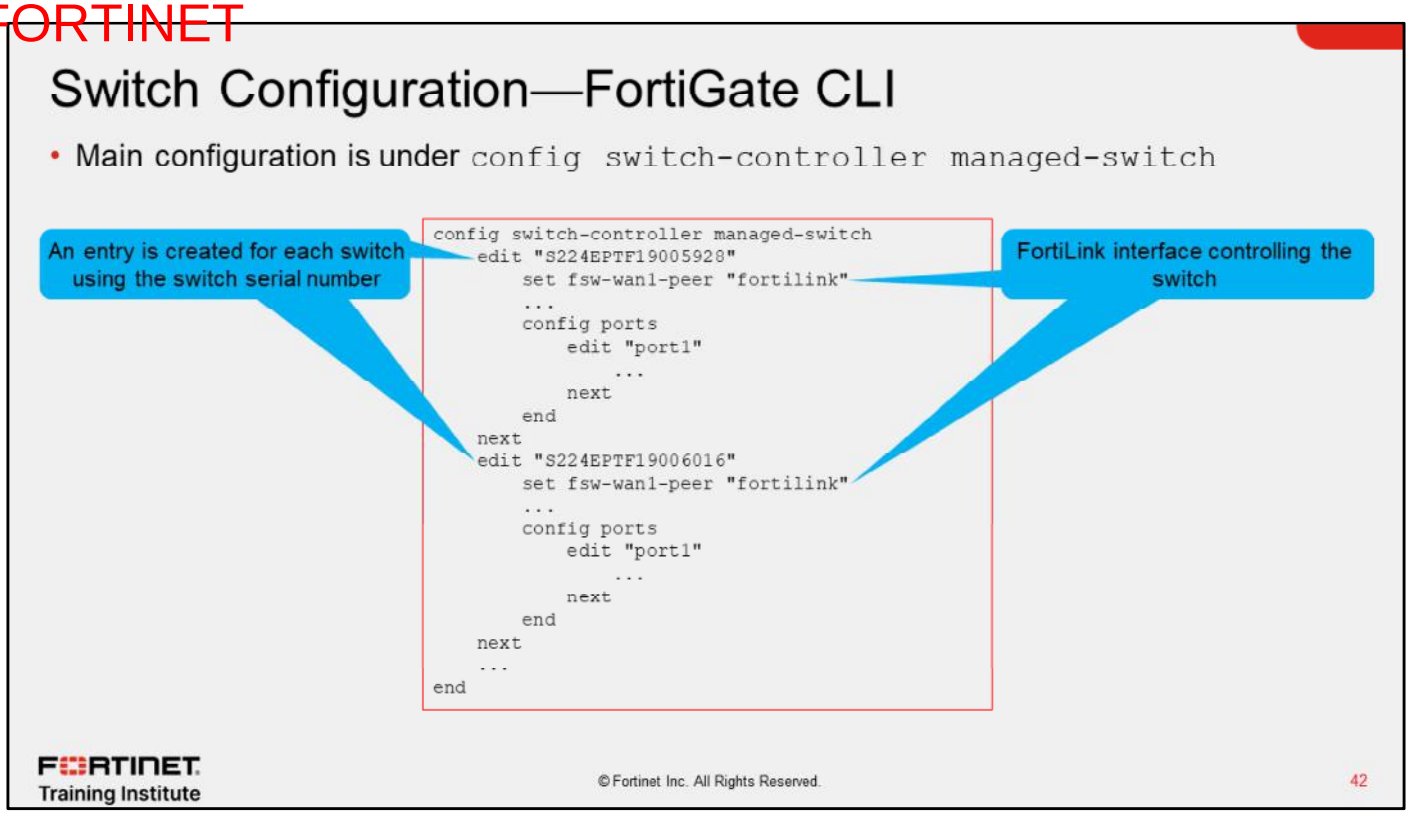
The FortiGate GUI contains the **WiFi & Switch Controller** section menu, which provides you with the most common configuration options for managing FortiAP and FortiSwitch devices. The bottom half of the menu contains the following FortiSwitch management pages:

- **FortiLink Interface**: This is where you configure the FortiLink interface for your switch stack. By default, FortiOS creates the FortiLink interface named **fortilink**.
- **Managed FortiSwitches**: Click here to view the list of switches currently discovered or authorized by FortiGate. You can perform different actions on a switch, such as reboot, firmware upgrade, factory reset, and deauthorize.
- **FortiSwitch Ports**: This displays the list of ports and trunks available on the switch and their status. You can also shut down or bring up ports, adjust their VLAN, STP, and PoE settings, and so on.
- **FortiSwitch VLANs**: A FortiSwitch VLAN is essentially a FortiGate VLAN interface that is bound to a FortiLink interface. The VLAN is then used for Layer 3 routing on FortiGate and Layer 2 segmentation on FortiSwitch. Here, you can configure the FortiSwitch VLANs used by FortiGate and FortiSwitch.
- **FortiSwitch Port Policies**: This is where you configure profiles for enforcing 802.1X authentication on switch ports.

You will learn more about these configuration pages in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

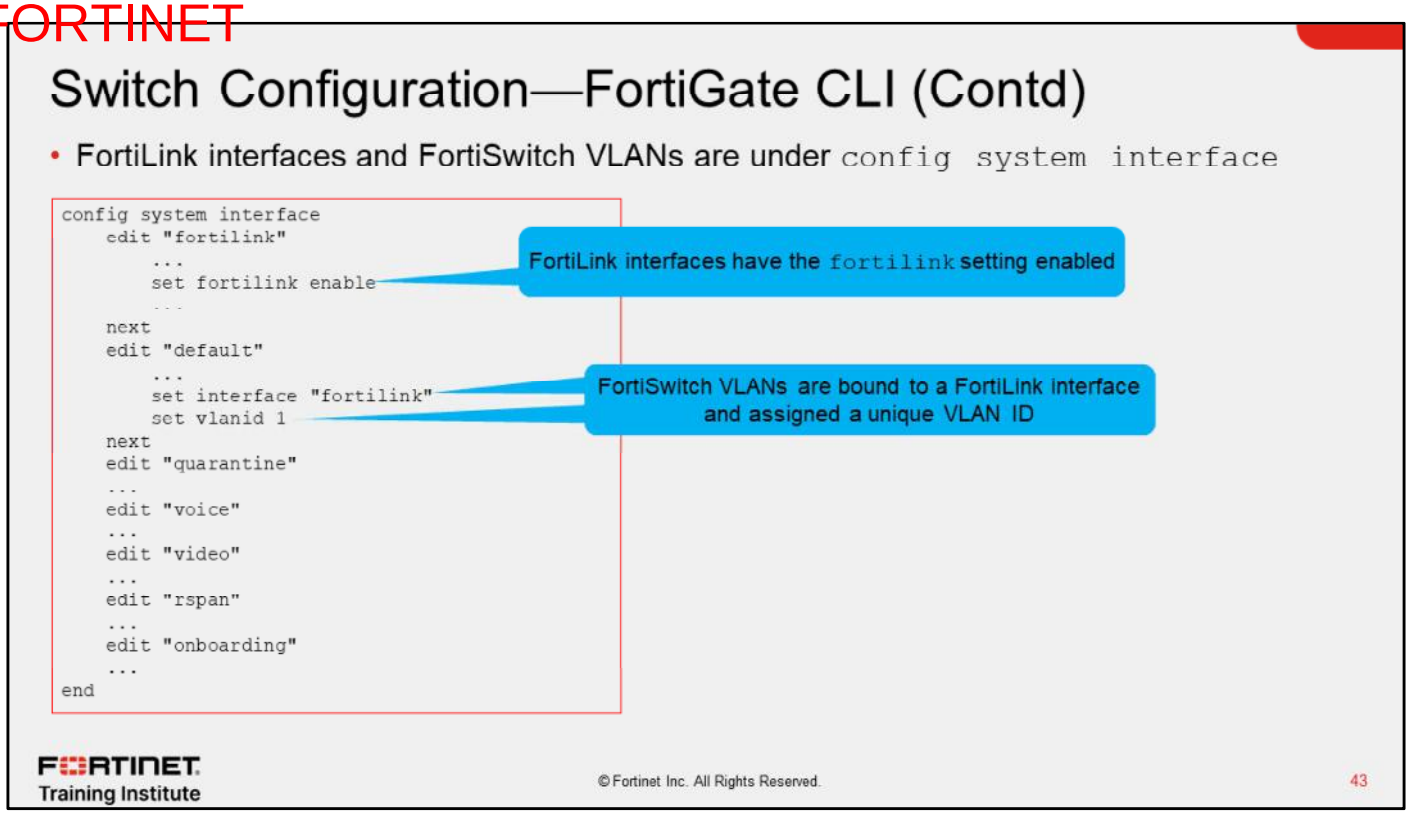


You may also need to use the FortiGate CLI to configure some settings for your managed switches, especially those that are not available on the FortiGate GUI.

The main configuration for your switch stack is found under `config switch-controller managed-switch`. Here, you will find an entry for every switch that was discovered by FortiGate. The entries are organized by serial numbers, and each entry indicates the FortiLink interface that the switch is connected to. In the example shown on this slide, both switches are connected to the default FortiLink interface. In addition, each entry displays the list of ports on the switch for which you can adjust multiple settings, such as VLANs, security profiles, STP settings, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

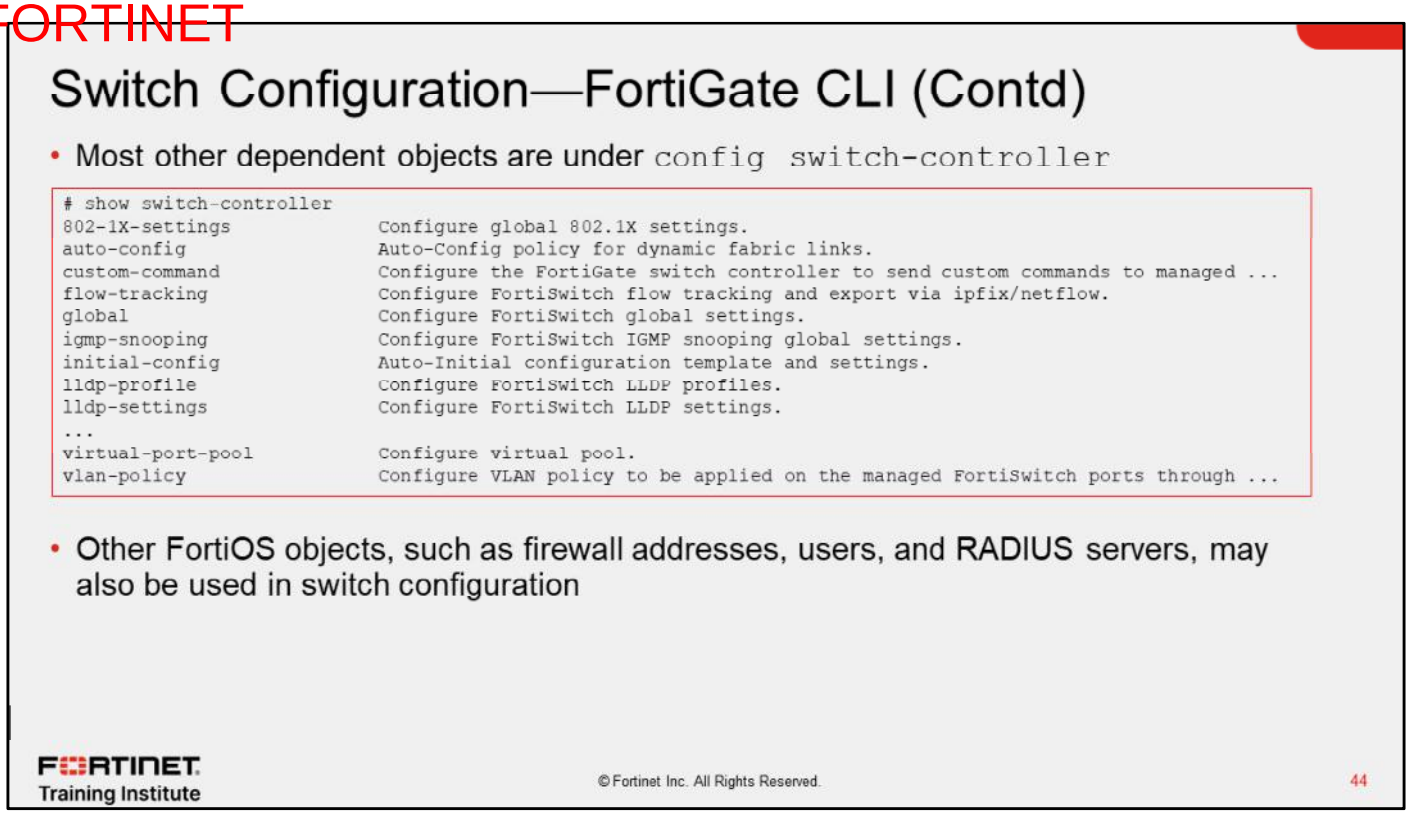


Another important part of the configuration of managed switches is found under `config system interface`. In addition to the FortiLink interfaces configured in the system, you will also find the different FortiSwitch VLANs created for your switch stack here.

The example on this slide shows some of the default FortiLink interface configuration, as well as some of the default FortiSwitch VLANs configuration. FortiSwitch VLANs must be bound to a FortiLink interface and assigned a unique VLAN ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

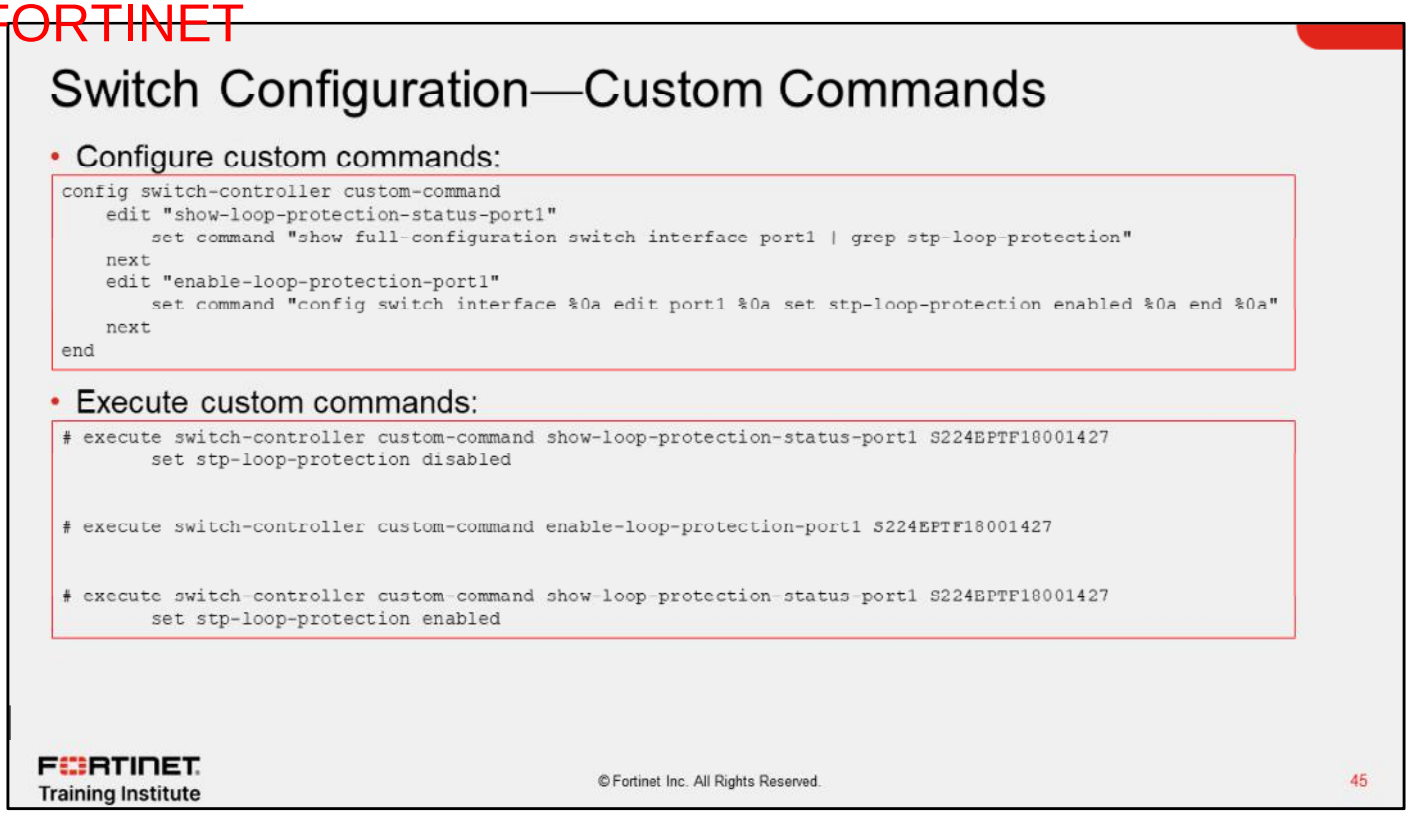


You may also need to configure dependent objects for your FortiSwitch devices. Most of these can be found in different locations under `config switch-controller`. The example on this slide shows some of the different configuration sections available under `config switch-controller`.

Note that some other FortiOS objects, such as firewall addresses, users, groups, and RADIUS servers, may also be used in the configuration for your switch. However, most of the configuration is likely to be found under the `config switch-controller` and `config system interface` sections.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



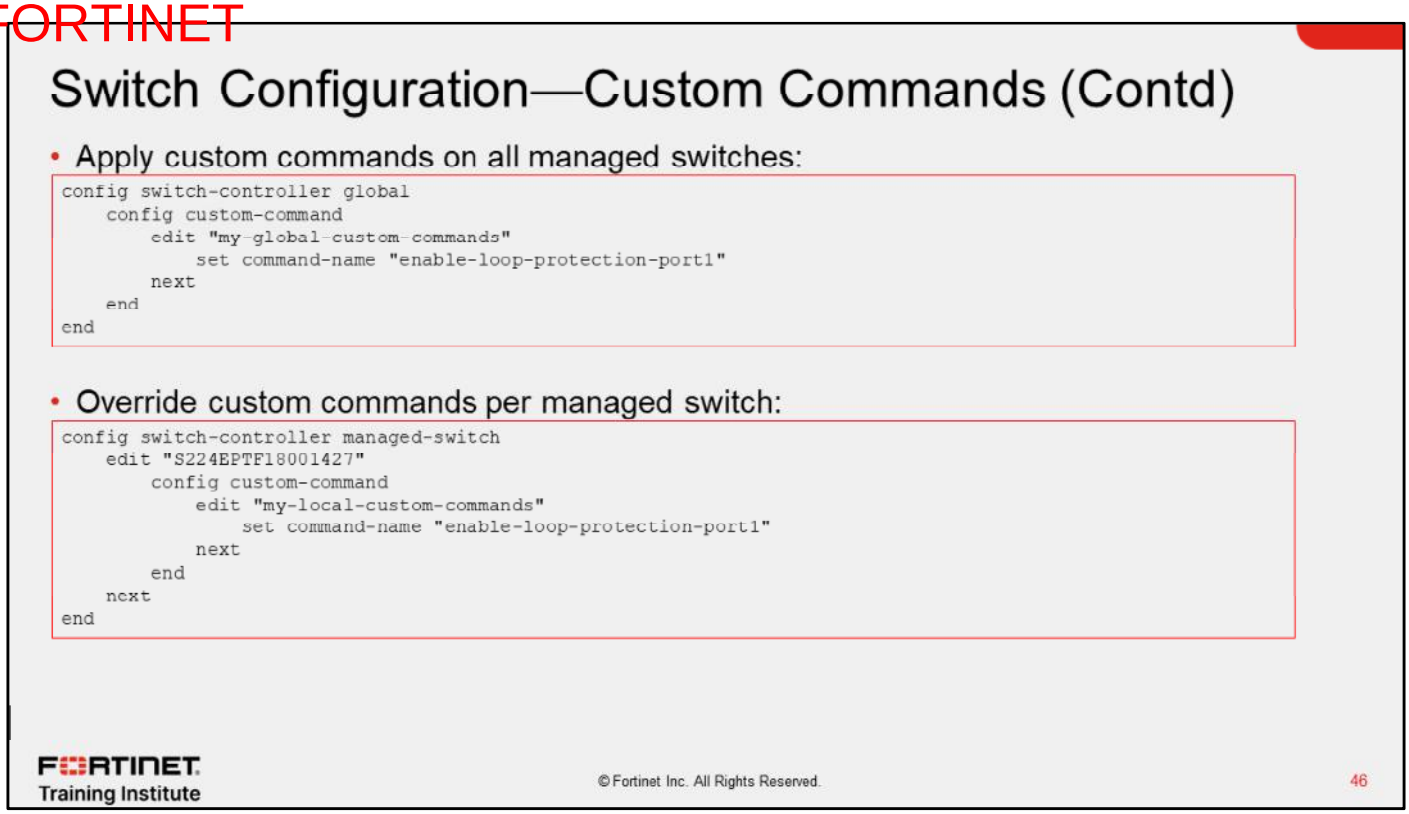
Some switch settings and diagnose commands are available on the FortiSwitch device only, and not on the FortiGate GUI or CLI. For these cases, you can either run the corresponding FortiSwitchOS command directly on FortiSwitch, or use the custom command feature on the FortiGate CLI to run the required commands on the switch.

The example on this slide shows how to configure and use the custom command feature to enable loop protection on port1 of a managed switch. Loop protection is available on the FortiSwitch GUI and CLI only, and enables a port to prevent loops that are not detected by Spanning Tree Protocol (STP). You will learn more about loop protection and STP in another lesson.

Note that for building a list of custom commands, the hexadecimal code `0a` is placed at the end of each command to mark the line breaks in the list. Also note that any output that is produced when executing the custom commands is displayed on the FortiGate CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

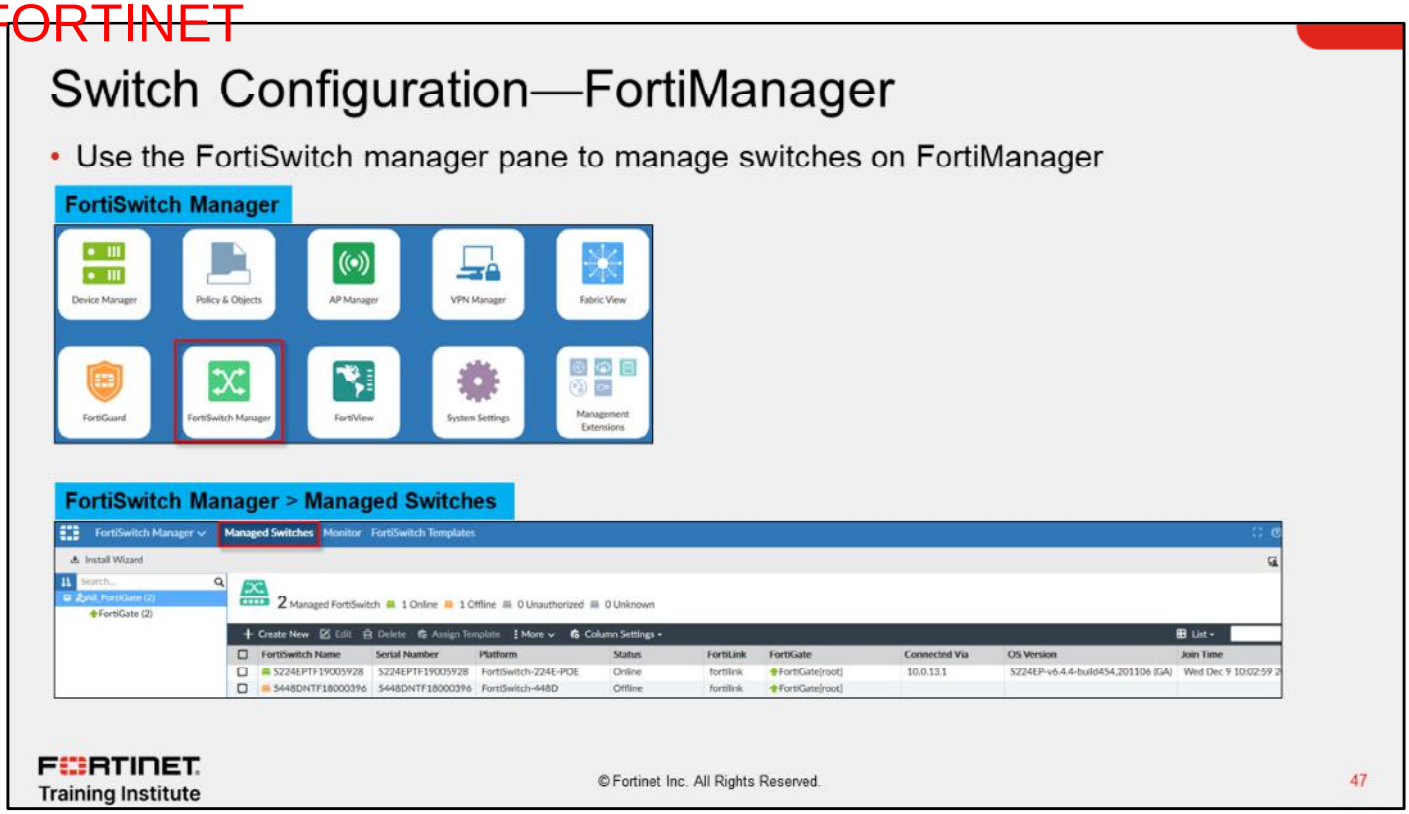
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also configure global custom commands that run when a switch is authorized, as shown in this slide. Alternatively, you can override the custom commands per switch, as shown in this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



On FortiManager, the FortiSwitch devices that are discovered by a managed FortiGate are also learned by FortiManager and displayed on the **FortiSwitch Manager** pane.

FortiSwitch manager enables you to centrally manage FortiSwitch devices discovered by all authorized FortiGate devices on FortiManager. Instead of accessing each FortiGate device to manage its attached FortiSwitch devices, you can manage all FortiSwitch devices controlled by all FortiGate devices from a single pane on FortiManager. This can considerably reduce the operating expenses from your network, especially for large networks that have tens or hundreds of switches deployed.

When you access the **FortiSwitch Manager** pane, you land on the **Managed Switches** page by default. This page displays a table containing all switches discovered by all FortiGate devices registered on FortiManager. For each authorized switch, the page displays the name, serial number, model (or platform), controlling FortiGate and VDOM, IP address (connected via), OS version, and join time. This is the same information that you would see on the FortiGate GUI for a switch. Each switch also displays an icon to the left of its name that reports its current status, which is obtained by FortiManager by polling the FortiGate REST API every three minutes. The different statuses mean:

- **Online**: The switch is authorized and the management link with FortiGate is up.
- **Offline**: The switch is authorized but the management link with FortiGate is down.
- **Unauthorized**: The switch was discovered by FortiGate, but it has not been authorized.
- **Unknown**: The switch is authorized but its status cannot be determined. This is usually the case when the controller (FortiGate) is offline.

This course focuses on switch management from FortiGate only, and therefore, does not describe switch management from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What portion of the configuration is pushed to FortiSwitch after the switch status changes from offline to online?
   - ✓ A. The delta configuration, if any changes were made
   - B. The complete configuration

2. What protocol does FortiGate use to push a configuration to FortiSwitch?
   - ✓ A. HTTPS
   - B. CAPWAP

3. Which statement about the configuration on a managed switch is true?
   - A. Changes made on FortiSwitch are synced to FortiGate.
   - ✓ B. Changes made on FortiGate are synced to FortiSwitch.

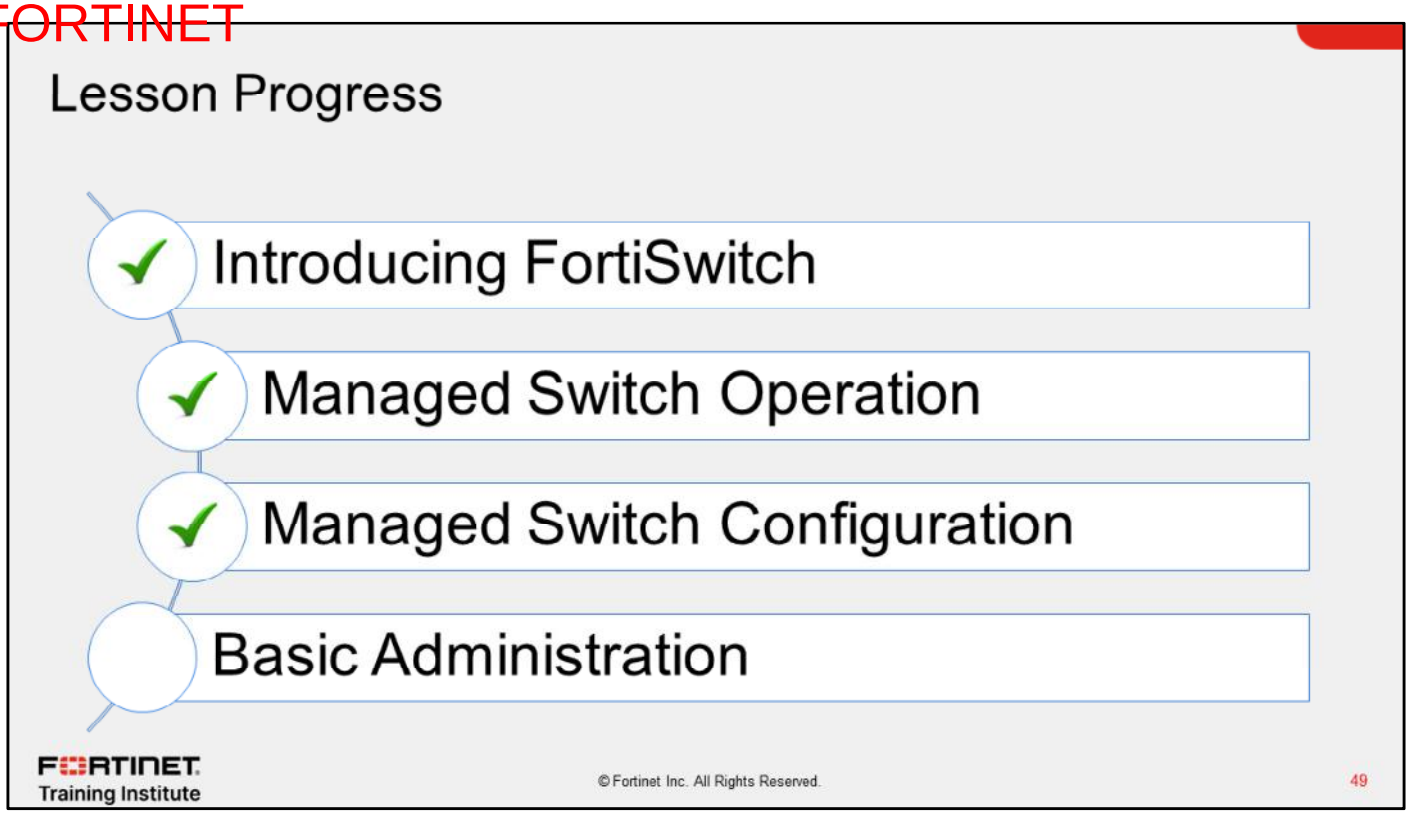
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

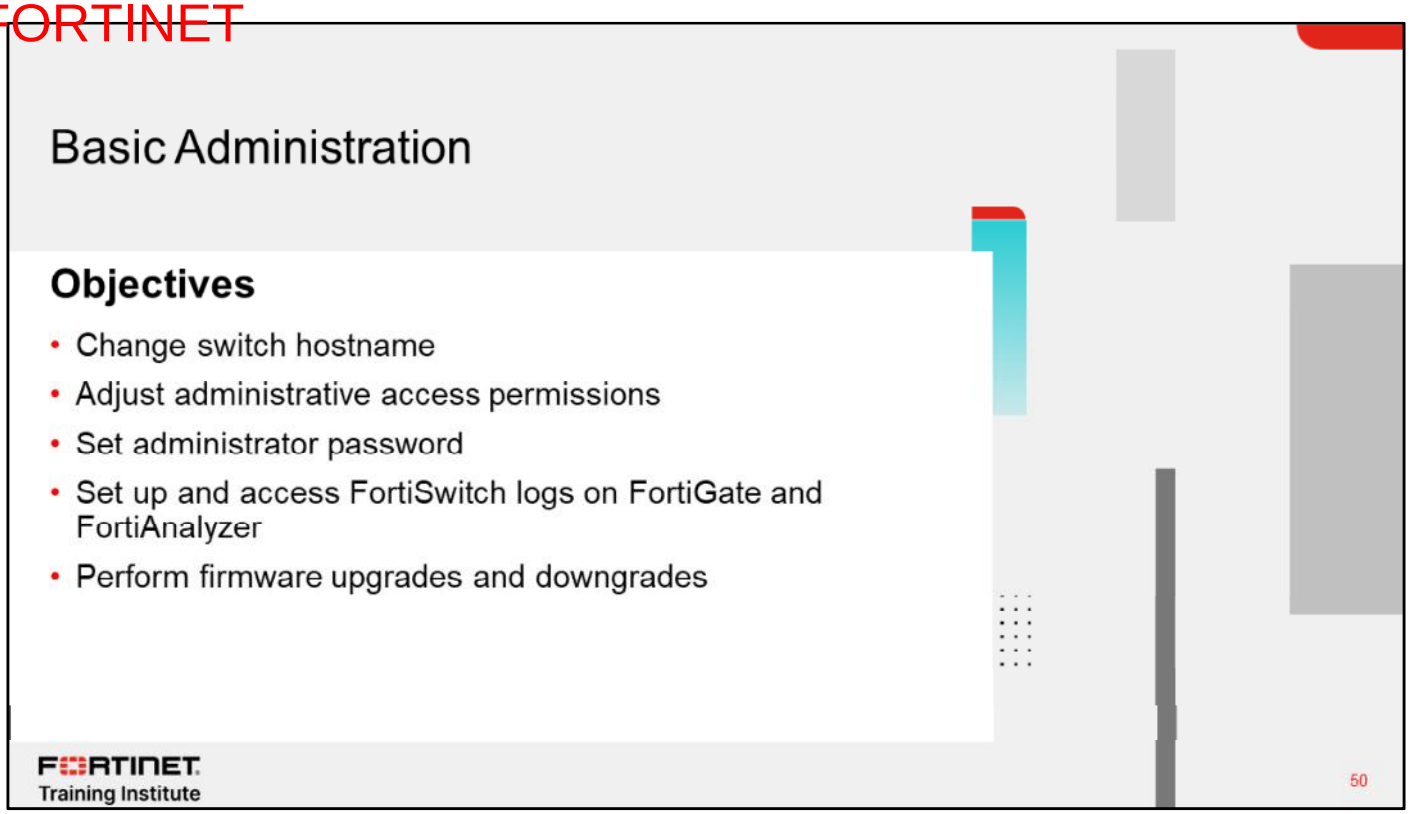


Good job! You now understand managed switch configuration.

Now, you will learn about basic administrative tasks on a switch operating in managed mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

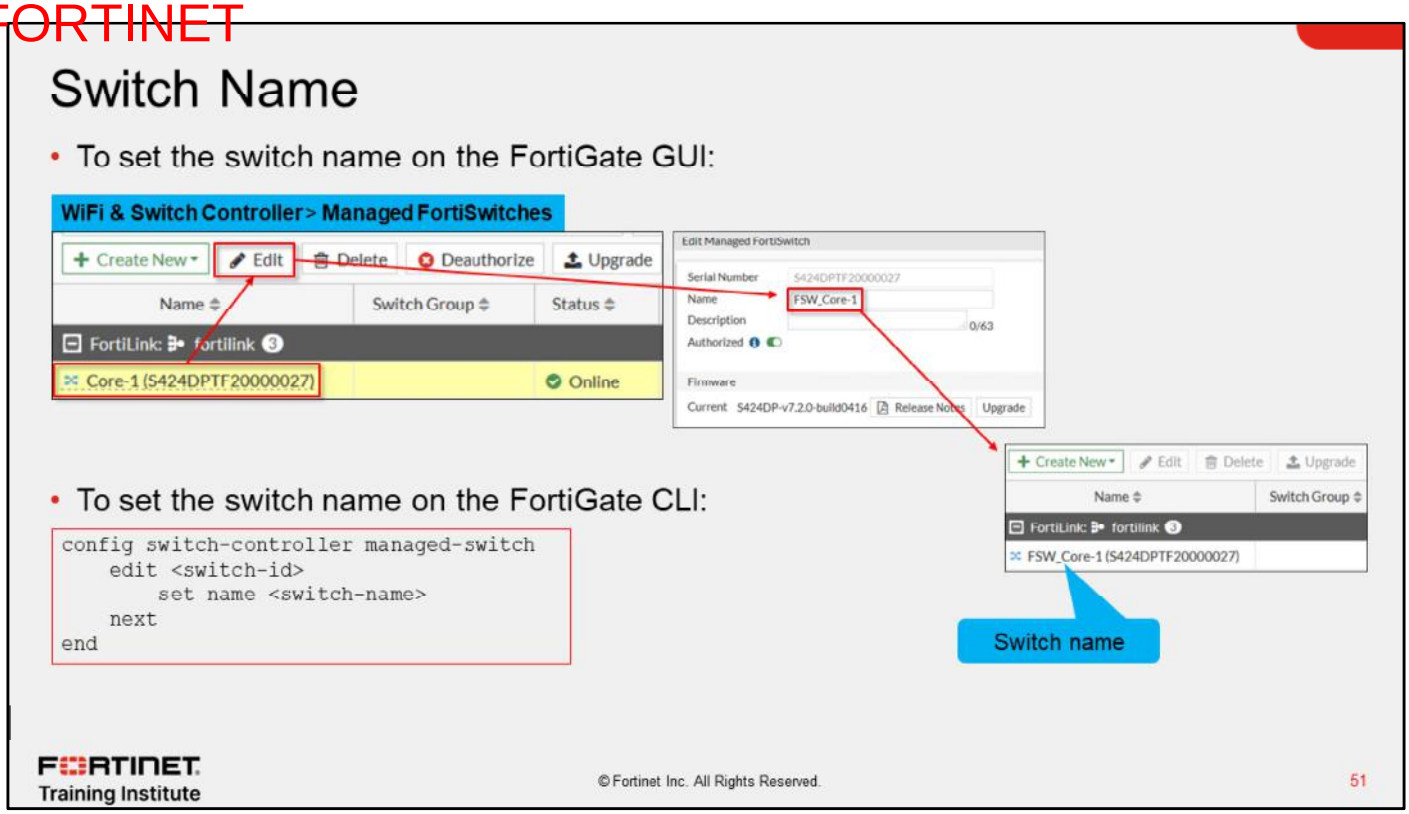


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic administration, you will learn about some basic administrative tasks you can perform on FortiSwitch when it is operating in managed switch mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



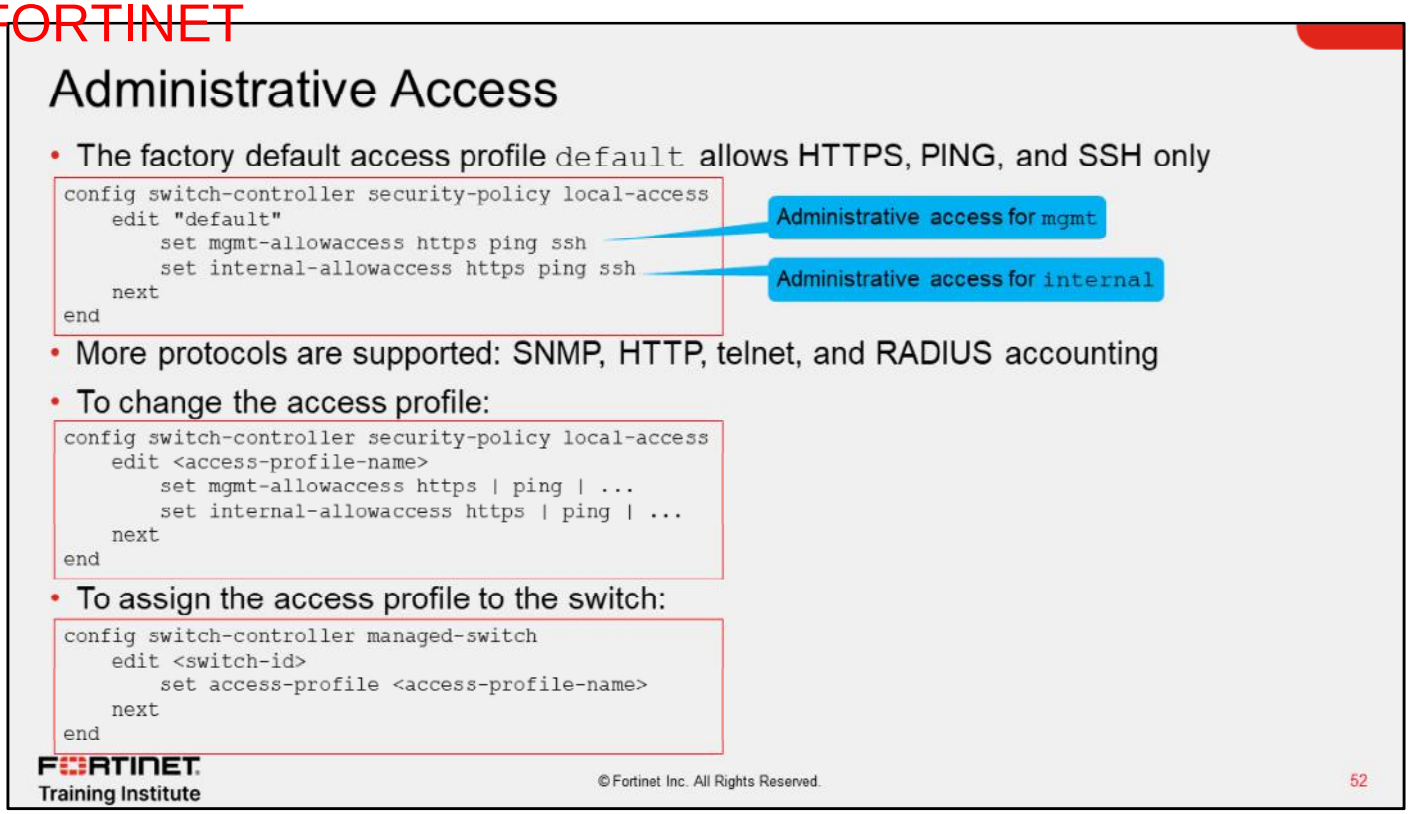
One of the first basic configuration changes you may want to perform is setting a descriptive name for your switch. Usually, you want to set a name that describes the device type and its role in the network.

On the FortiGate GUI, you can find the switch name setting after you select the switch on the **Managed FortiSwitches** configuration page, and then click **Edit**. On the FortiGate CLI, you use the `name` setting to configure the switch name.

After you configure the switch name, the name appears on the **Managed FortiSwitches** configuration page automatically.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

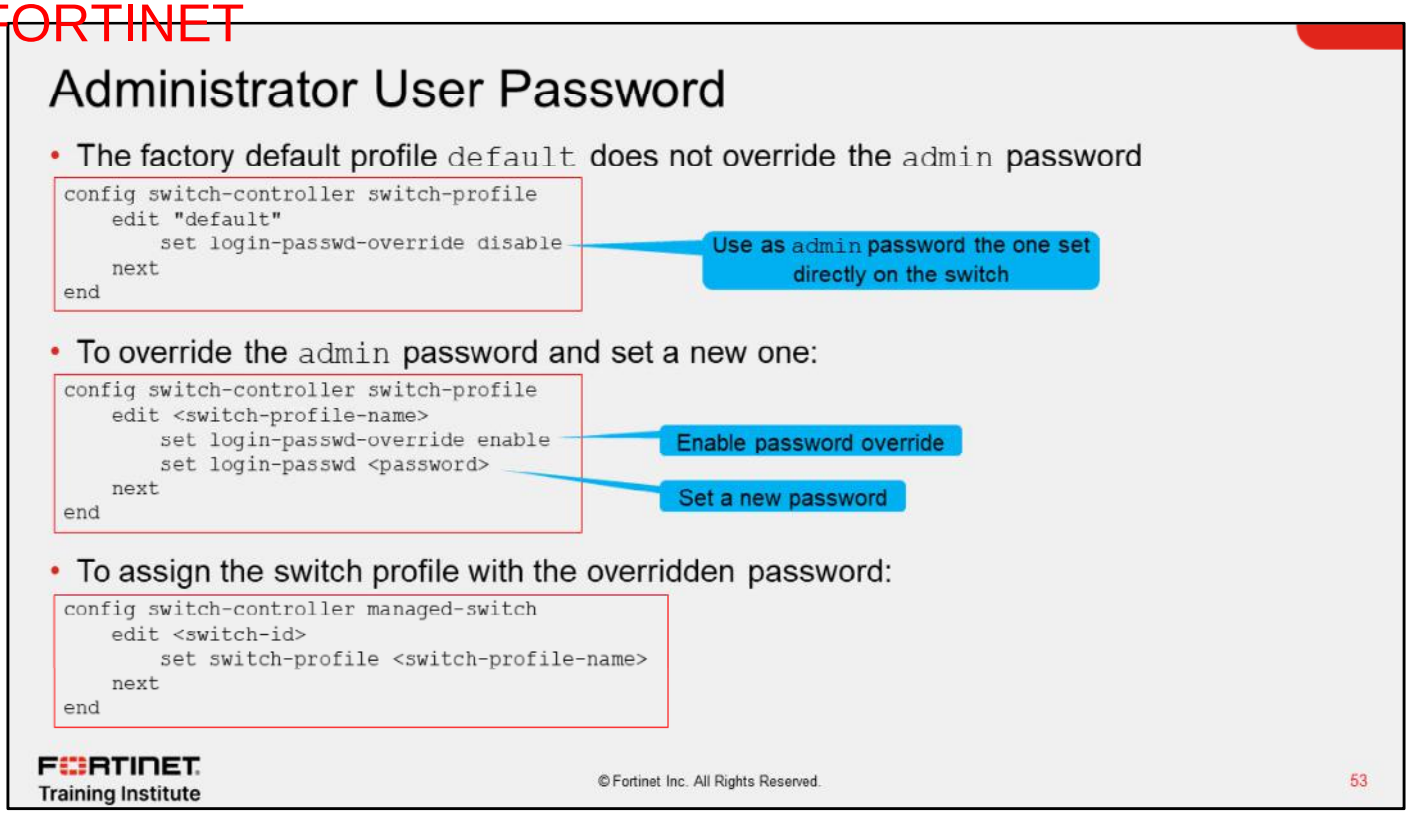


The administrative access on a managed switch is controlled by the access profile assigned to the switch. A factory default access profile named `default` is assigned to the switch after it is authorized on FortiGate. The `default` access profile has HTTPS, PING, and SSH administrative access enabled for both the `mgmt` and `internal` interfaces.

If you need to edit the administrative access on a switch, you must create a new access profile and assign it to the switch, or edit the existing default access profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

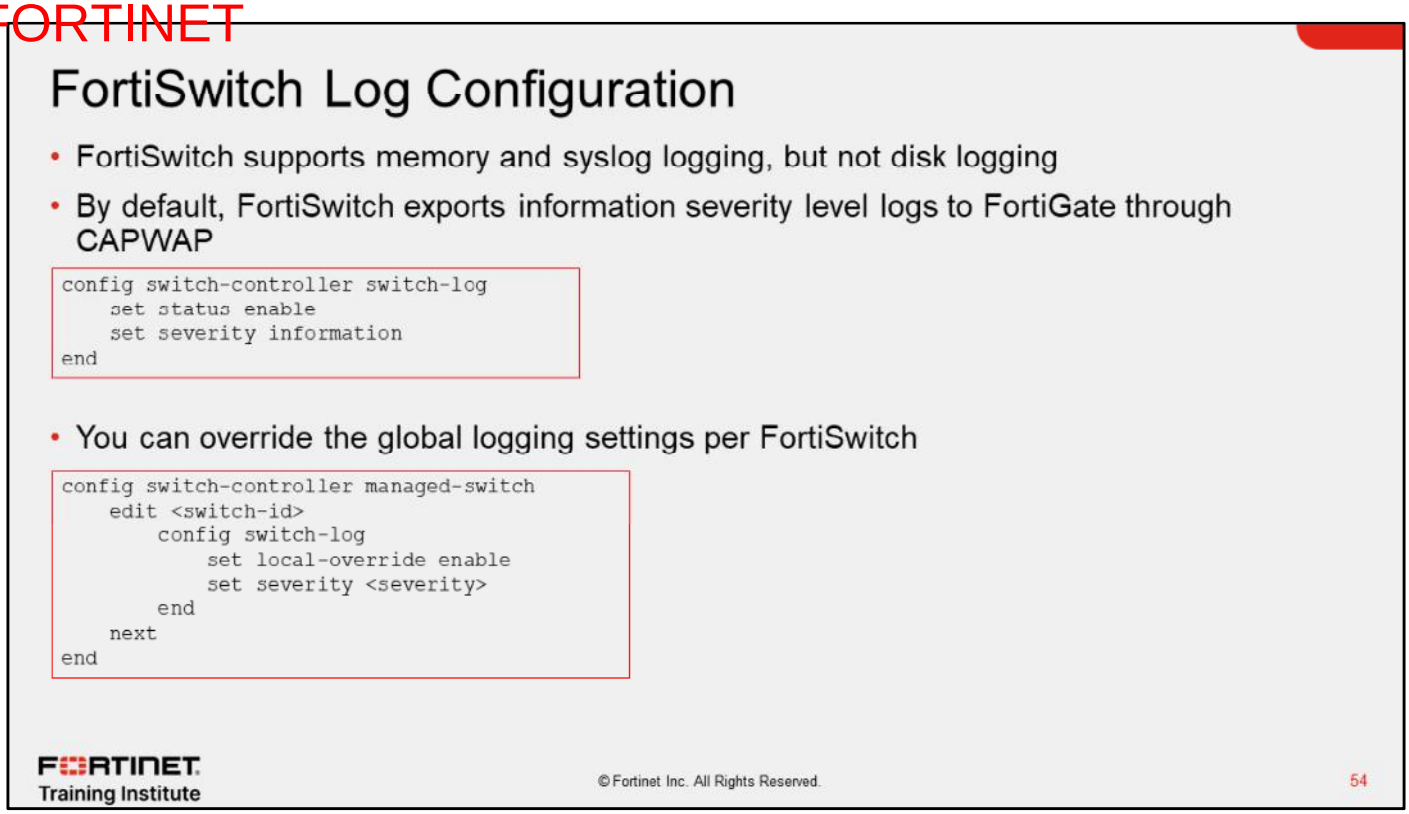


The admin password on a managed switch is controlled by the switch profile assigned to the switch. A factory default switch profile named default is assigned to the switch after it is authorized on FortiGate. The default switch profile does not change the admin user password set locally on the switch.

If you need to override the admin password set locally on the switch and replace it with a different password, you must create a new switch profile and assign it to the switch, or edit the existing default switch profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



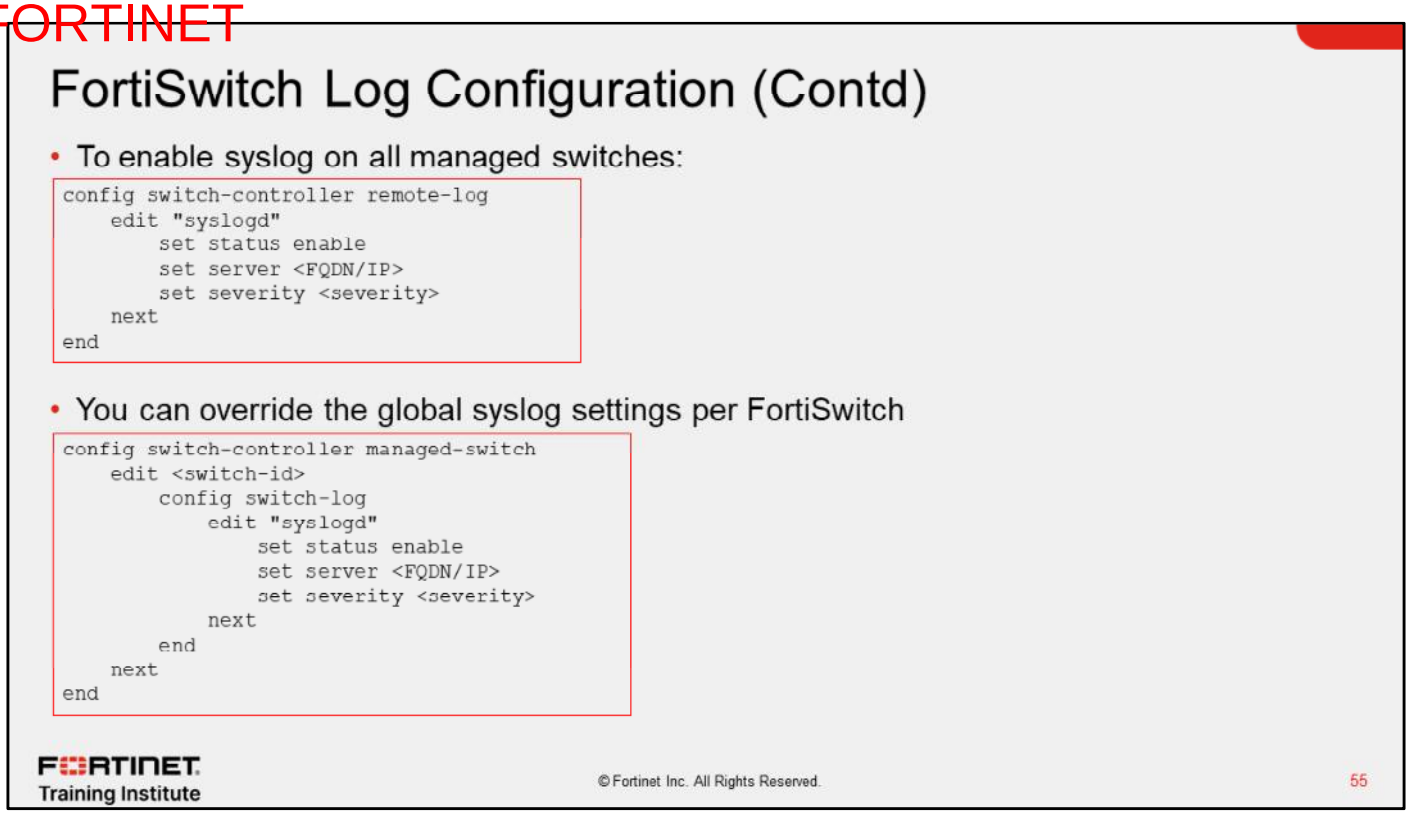
FortiSwitch supports memory and syslog logging only. FortiSwitch does not support disk logging.

Memory logging is enabled by default on FortiSwitch. However, when logging to memory, the amount of space allocated to logs is very small, and a switch reboot results in the removal of all logs stored in memory. For this reason, when you manage a switch on FortiGate, the switch also exports the logs to FortiGate so they can be stored on the FortiGate and displayed on the GUI. FortiSwitch sends its logs to FortiGate through CAPWAP. FortiGate then stores the FortiSwitch logs in all its enabled logging devices: memory, disk, FortiAnalyzer, and syslog.

Also, by default, FortiSwitch sends logs that are assigned a severity level of information or higher to FortiGate. You can set a different log severity level either globally or per FortiSwitch as shown on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

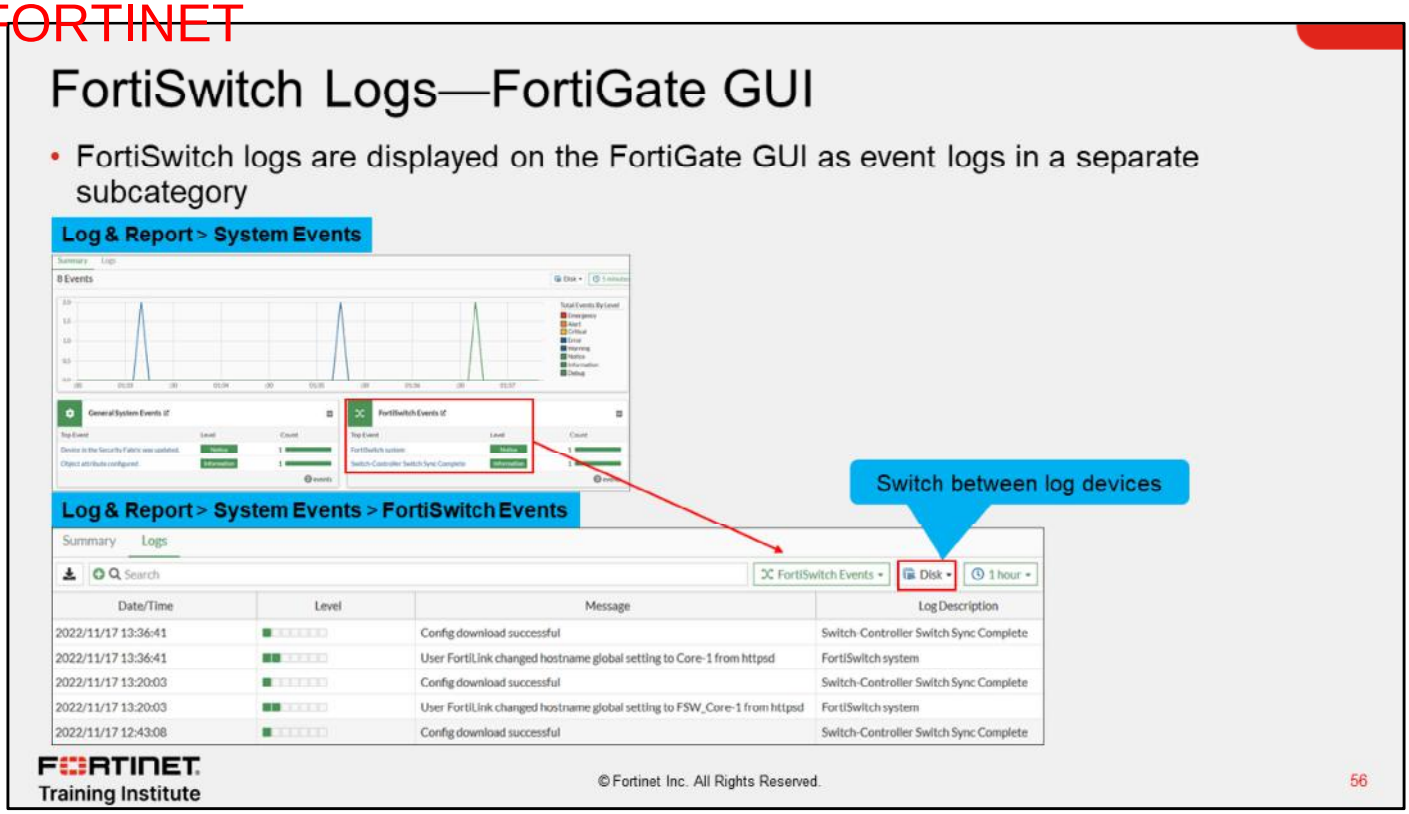
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can enable syslog on all managed switches or per switch on the FortiGate CLI, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

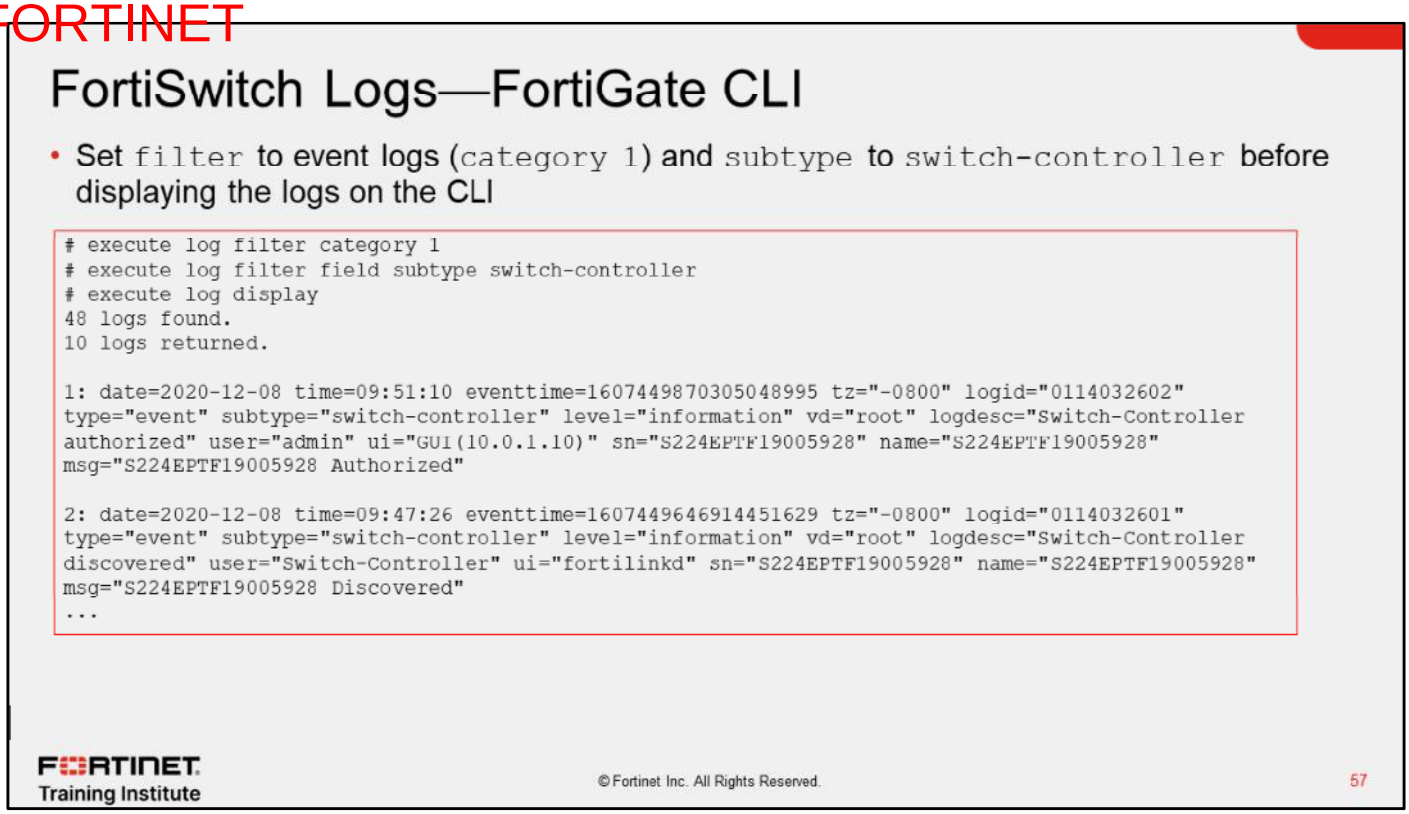
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows an example of some FortiSwitch logs displayed on the FortiGate GUI. FortiSwitch logs are available as event logs on the FortiGate GUI, under the **FortiSwitch Events** subcategory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



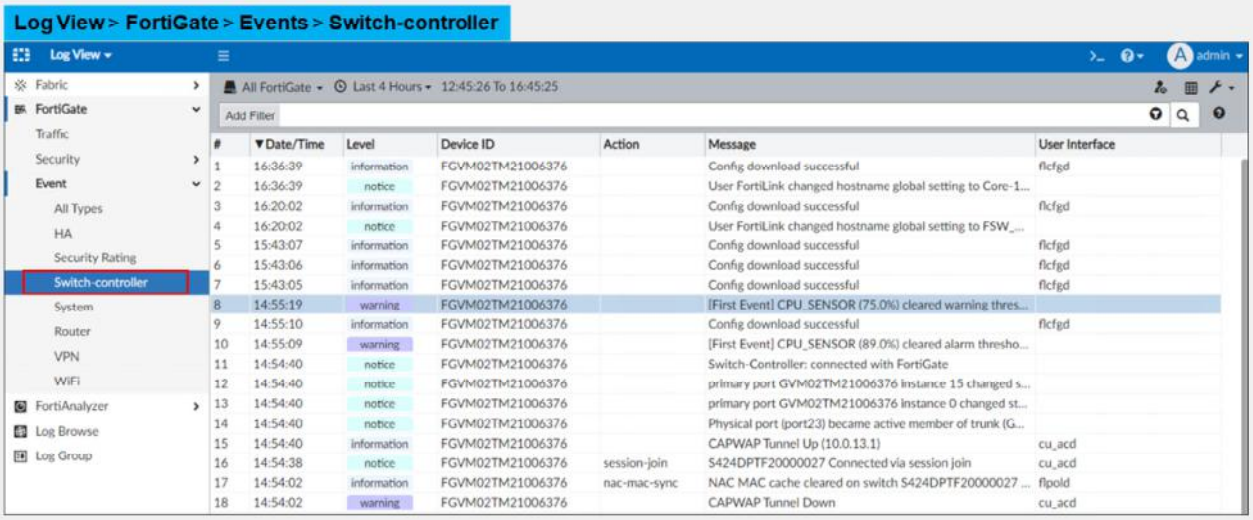
You can also display the FortiSwitch logs on the FortiGate CLI. Set `filter` to event logs (`category 1`) and `subtype` to `switch-controller`. The example on this slide shows how to set up the filter and display the logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSwitch Logs—FortiAnalyzer

- FortiSwitch logs are displayed on the FortiGate GUI as events logs in a separate category



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
58

The example on this slide shows some FortiSwitch logs displayed on FortiAnalyzer. FortiSwitch logs are available as event logs in the **Log View** pane, under the **Switch-controller** subcategory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Firmware Upgrade—FortiGate GUI

- Use the firmware upgrade tool on the GUI



- Change the firmware upgrade method (enable = HTTPS, disable = CAPWAP)

```
config switch-controller global
    set https-image-push enable | disable
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

59

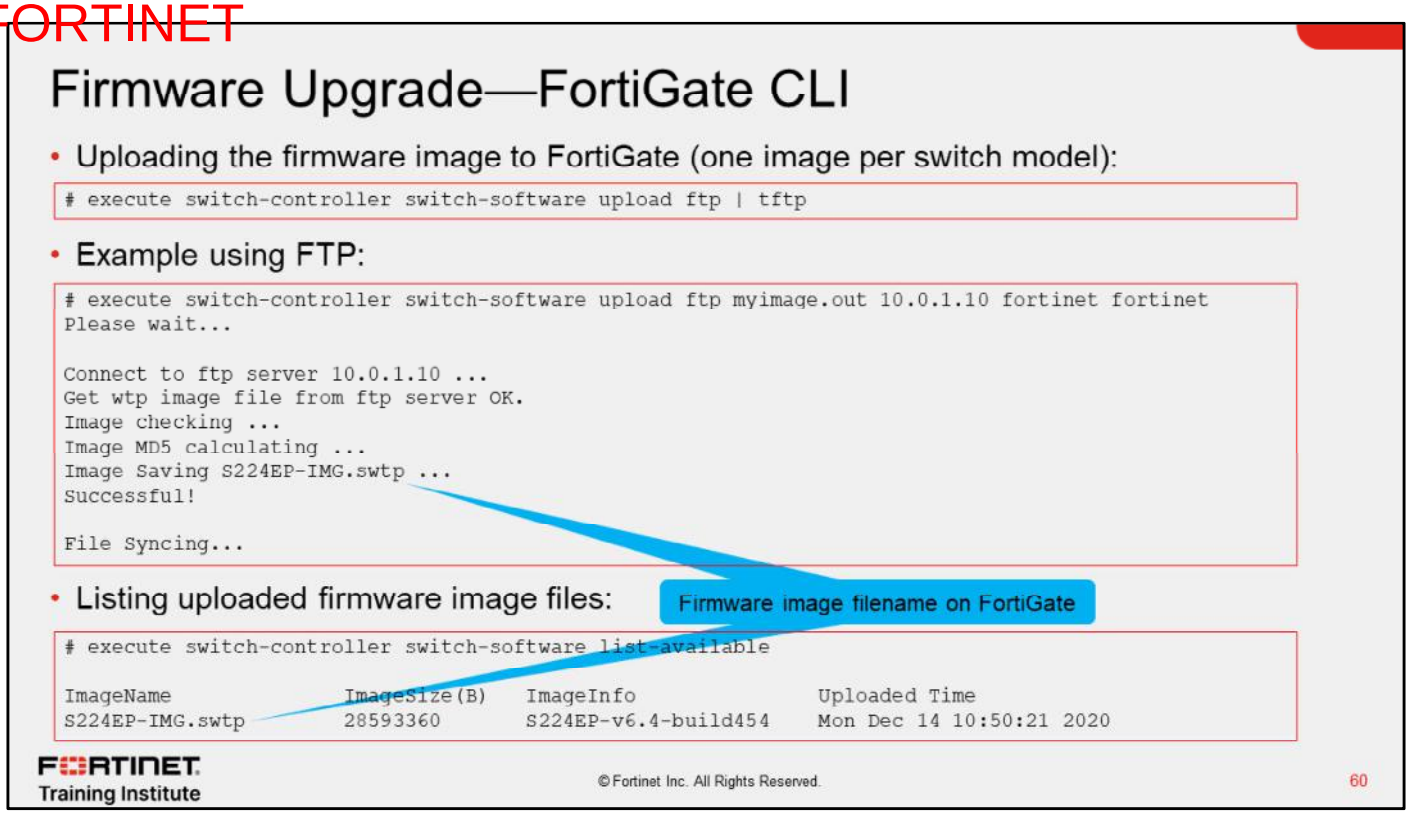
You can upgrade the firmware on a switch using the FortiGate GUI by going to the **Managed FortiSwitches** page, selecting the target switch, and then clicking the **Upgrade** button. Then, you can choose to have FortiGate download the firmware upgrade file from FortiGuard or upload your local firmware image.

After FortiGate starts pushing the firmware image to the switch, the switch status shows **Image Downloading**. After the switch receives the file, the switch reboots as part of the firmware upgrade process. As a result, you will notice the switch status changing to **Offline**, and then back to **Online** after it finishes the upgrade process and joins the switch controller again.

The default firmware upgrade method is HTTPS. You can also use CAPWAP as an alternative upgrade method. HTTPS is recommended because of its higher scalability and performance, and is supported as of FortiSwitchOS 3.6.1. If your switch is running a FortiSwitchOS version older than 3.6.1, you can change to CAPWAP by disabling the CLI setting shown on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

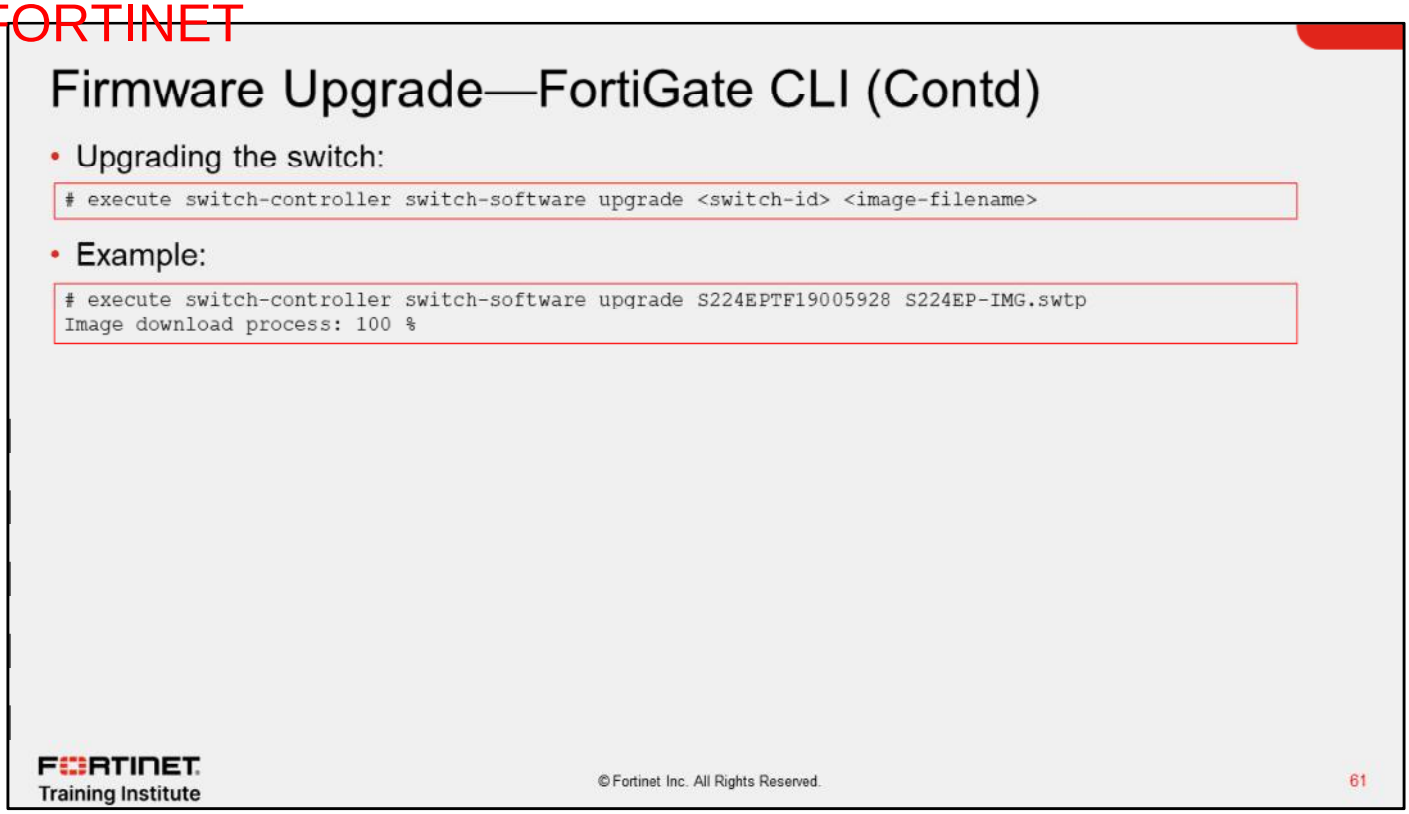


You can also upgrade the firmware of a switch on the FortiGate CLI. For this, you must first upload the target firmware image to FortiGate from an FTP or TFTP server. Note that FortiGate can store only one image per switch model. This means that if you upload another image for the same switch model, FortiGate overwrites the existing one. In addition, when saving the firmware image file, FortiGate saves the file under a different name than the original filename.

The example on this slide shows how you can use the FortiGate CLI to upload a firmware image using FTP, and how you can get the list of all switch firmware image files stored in FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

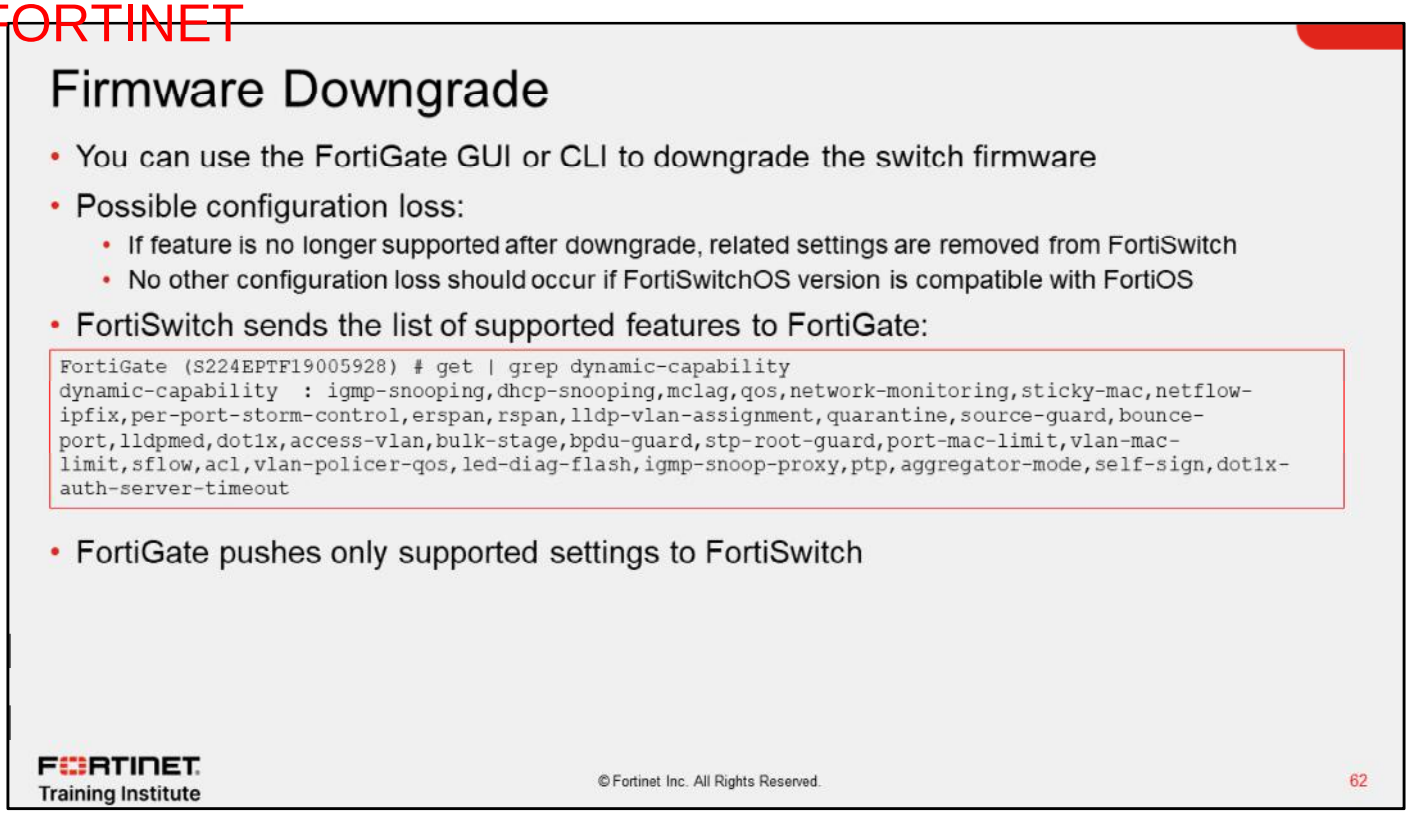
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you upload the firmware image to FortiGate, you can use the CLI command shown on this slide to upgrade the switch. Remember to use the filename used by FortiGate to store the firmware image locally and not the original filename.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can downgrade the firmware of your switch by using the FortiGate GUI or CLI in the same way you use them for upgrading the firmware.

After the firmware downgrade, the settings on the switch should not be lost, unless you downgrade the switch firmware to a version that does not support a feature that is being used, or if the target FortiSwitchOS version is not compatible with the FortiOS version.

In addition, FortiSwitch sends a list of its supported features to FortiGate. The list is displayed in the `dynamic-capability` CLI setting, which is read-only. When you configure a feature on FortiGate that the FortiSwitchOS version on a switch does not support, FortiGate does not push the related settings to that switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What are the administrative protocols that are enabled by default on a managed FortiSwitch?
   - A. HTTPS, telnet, and ping
   - ✓ B. HTTPS, SSH, and ping

2. What protocol does FortiSwitch use to export logs to FortiGate?
   - A. SSH
   - ✓ B. CAPWAP

3. What is the default log severity level used by FortiSwitch to export logs to FortiGate?
   - A. Warning
   - ✓ B. Information

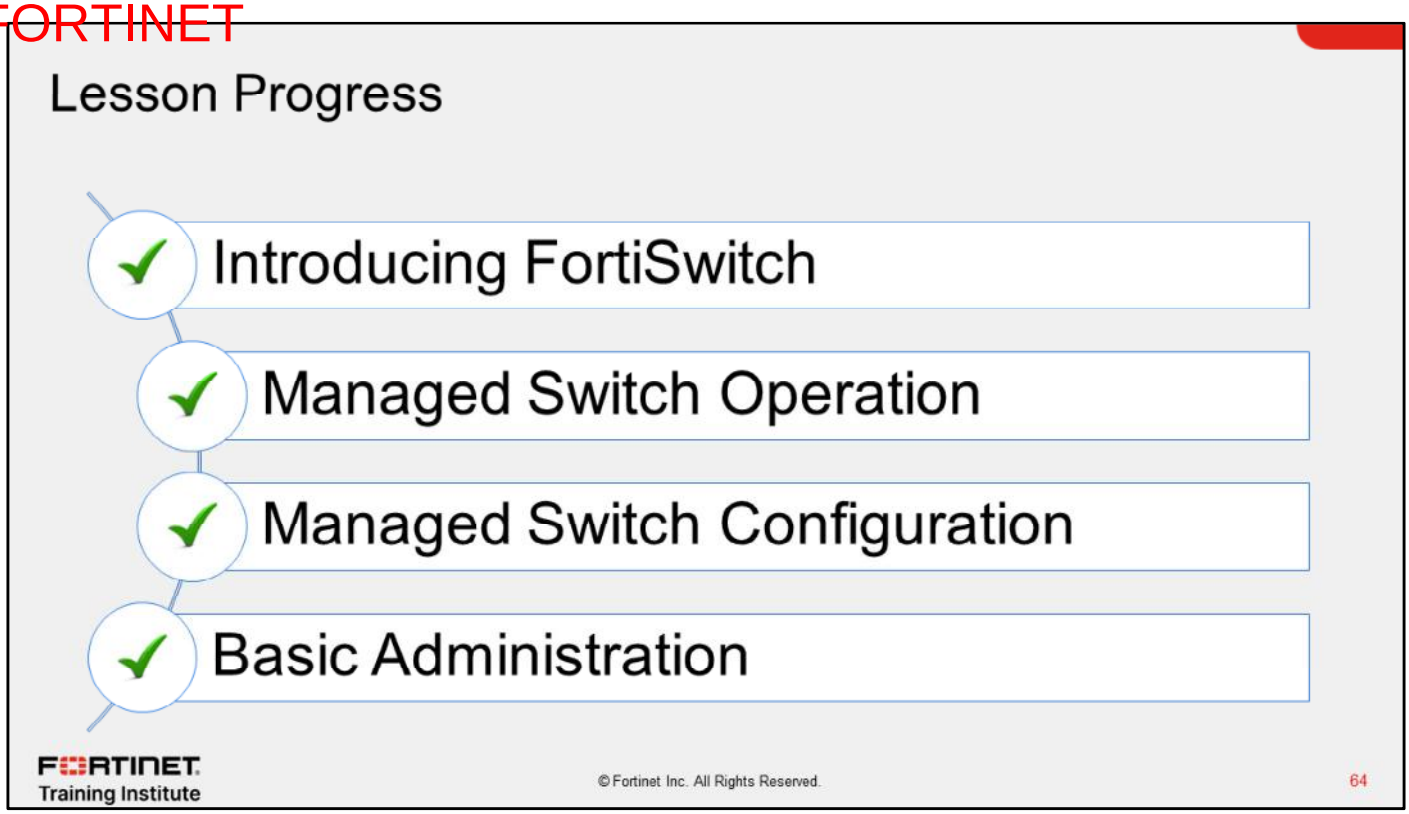
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

63

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

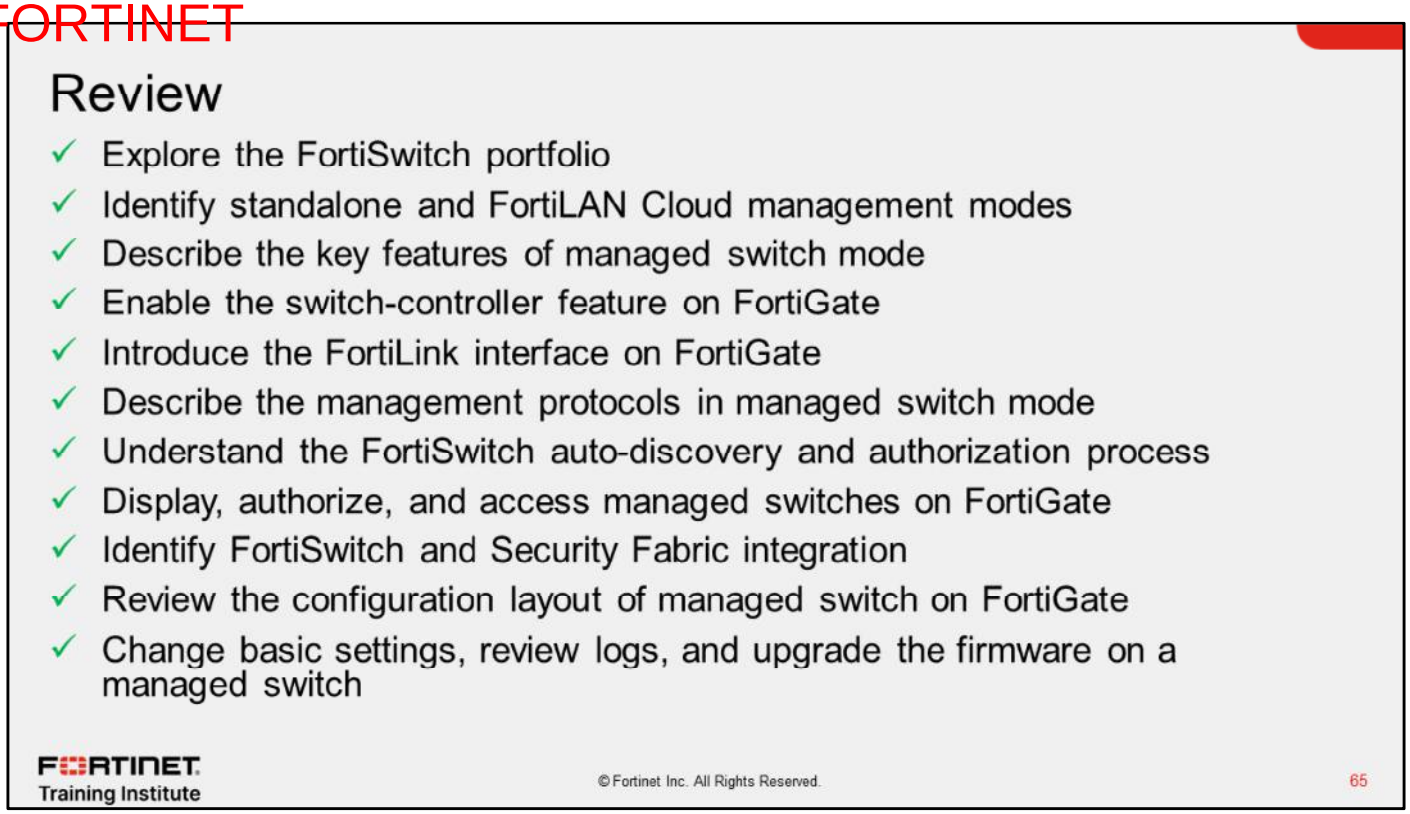


Good job! You now know how to perform basic administrative tasks on FortiSwitch working in managed switch mode.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

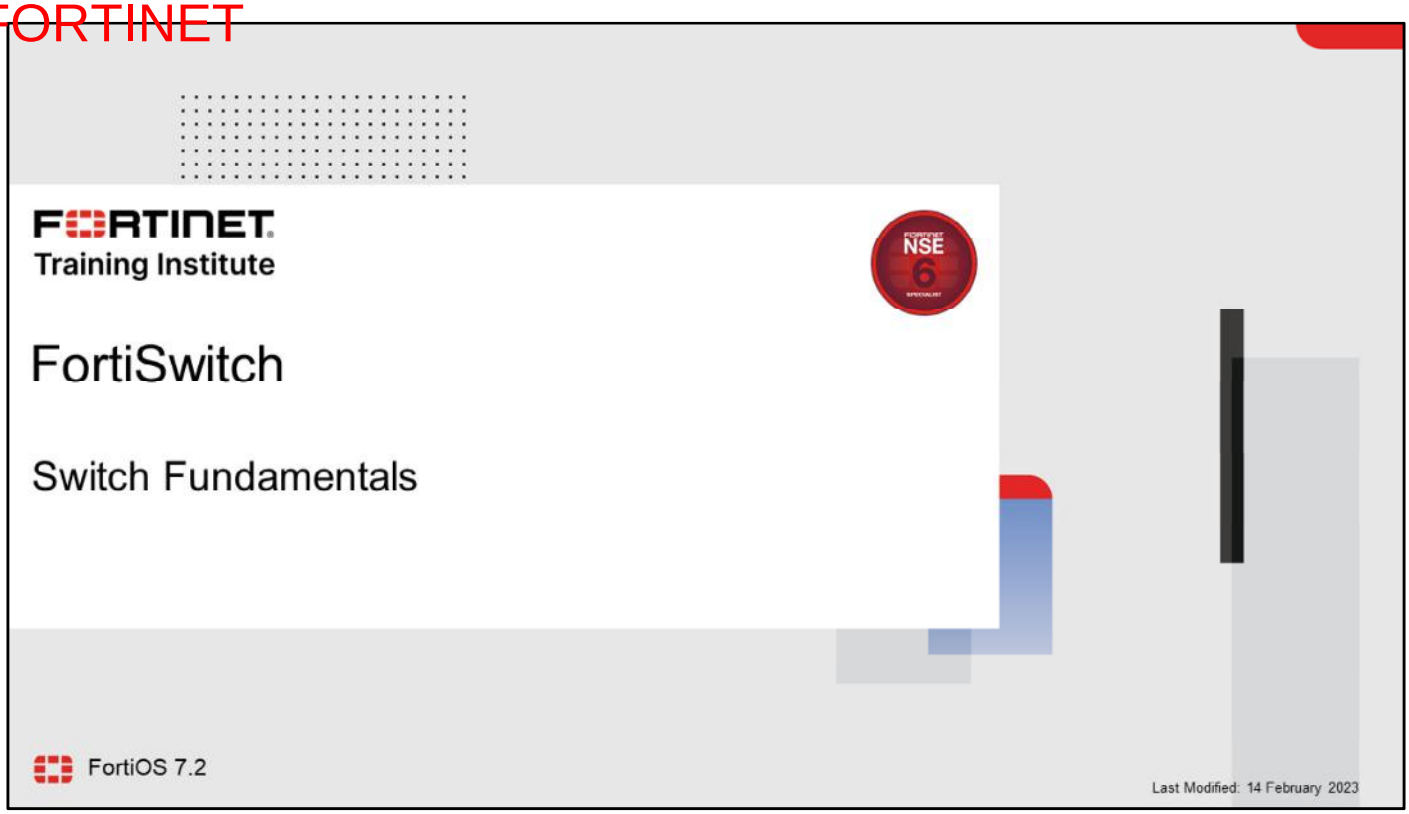


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about FortiSwitch, its management modes, key features, and basic operation.

Vouchers & Dumps are Available | WhatsApp +201224560923

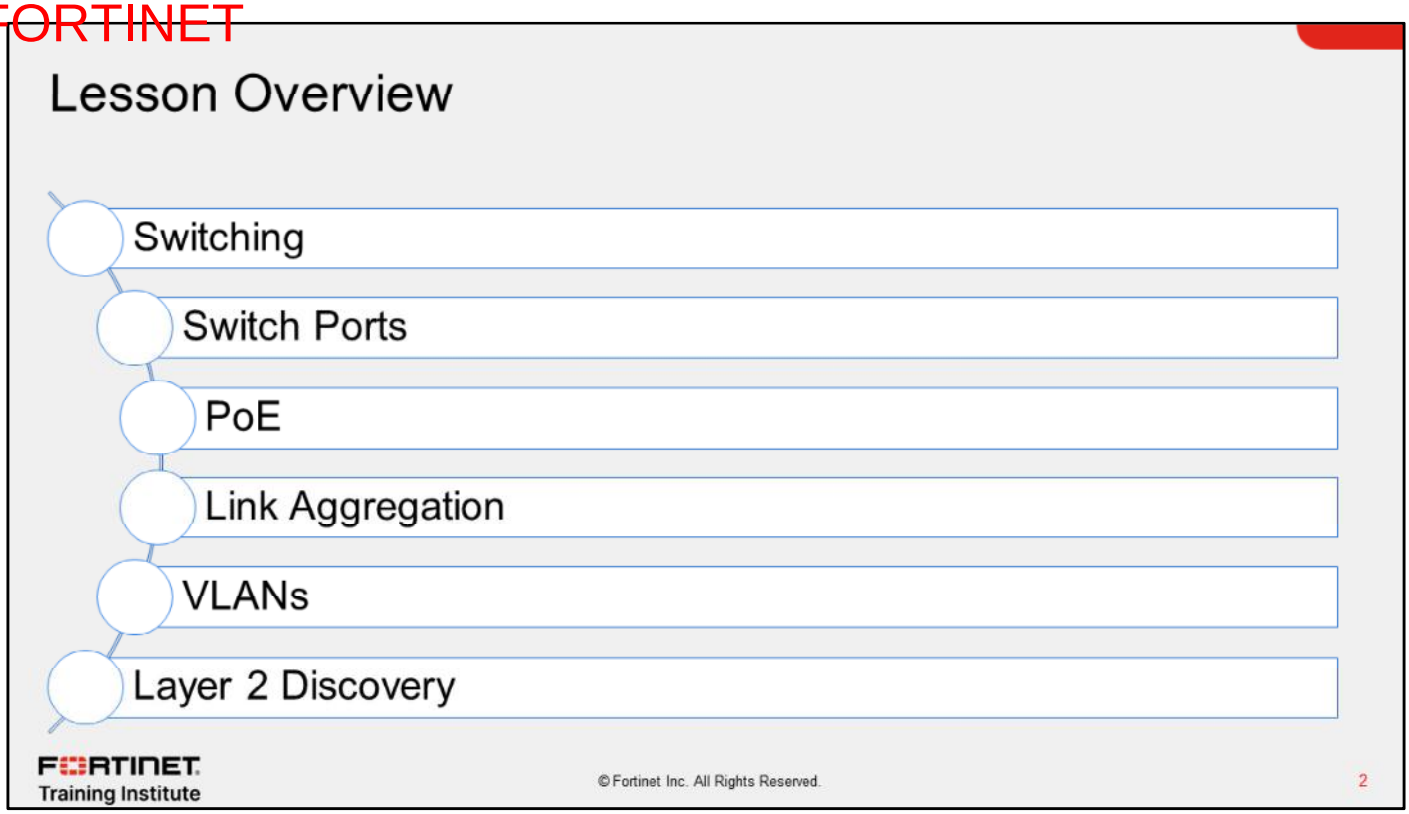
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSwitch essentials, focusing on the managed switch mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

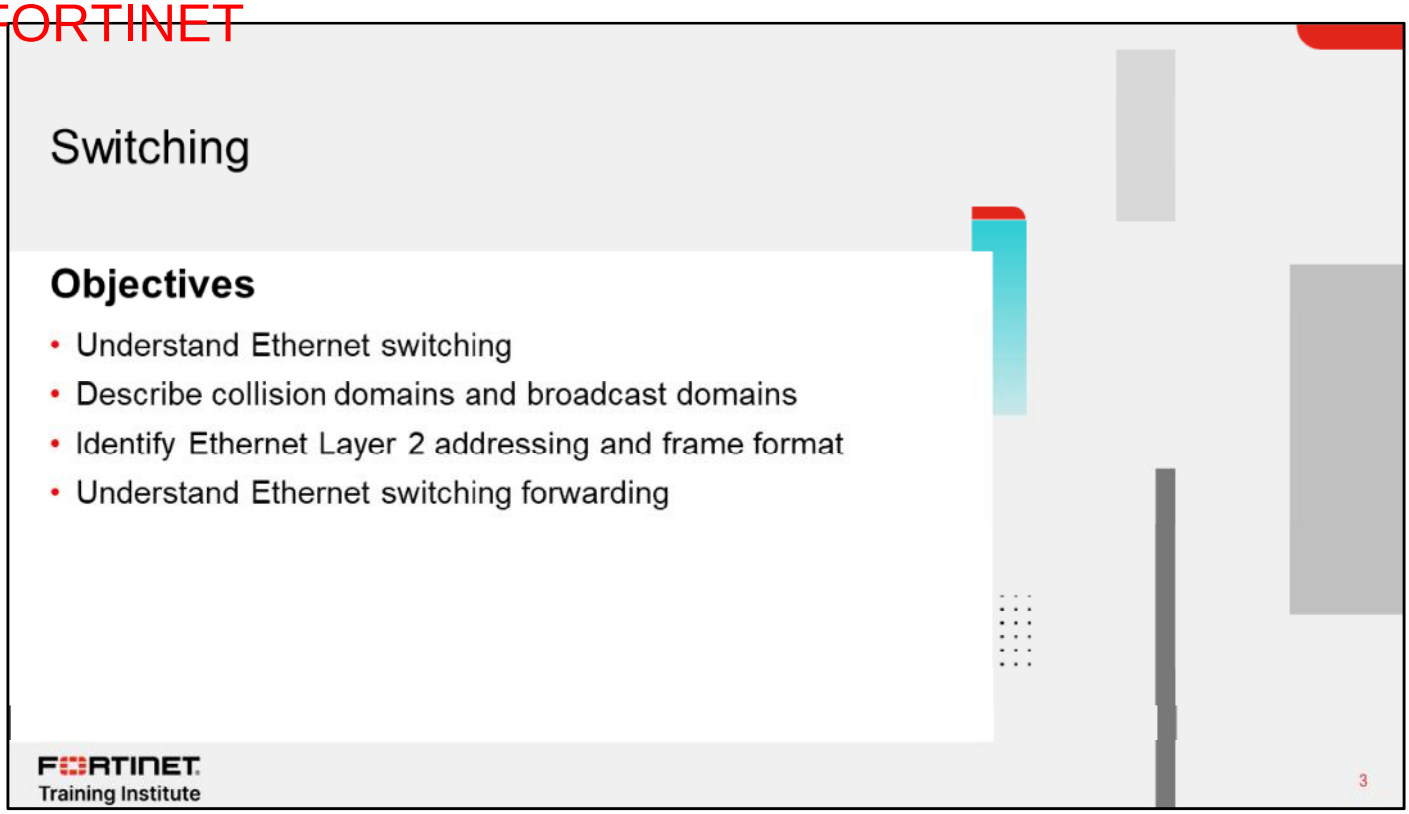
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

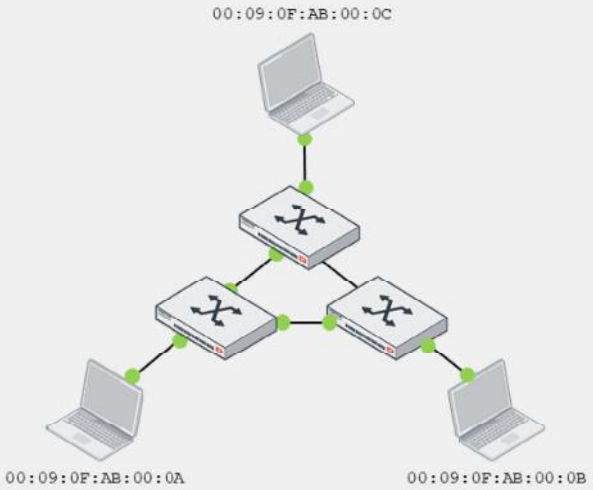
By demonstrating competence in Ethernet switching concepts and operation, you should be able to understand how FortiSwitch handles traffic in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is Ethernet Switching?

- Switches forward Ethernet frames based on their destination MAC address
  - MAC addresses identify NICs in the network
- Ethernet switches
  - Operate at Layer 2 of the OSI model
  - Learn MAC addresses and record them in MAC address tables
  - Are usually deployed in LANs
  - Provide high-performance connectivity
    - High bandwidth
    - Low latency



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

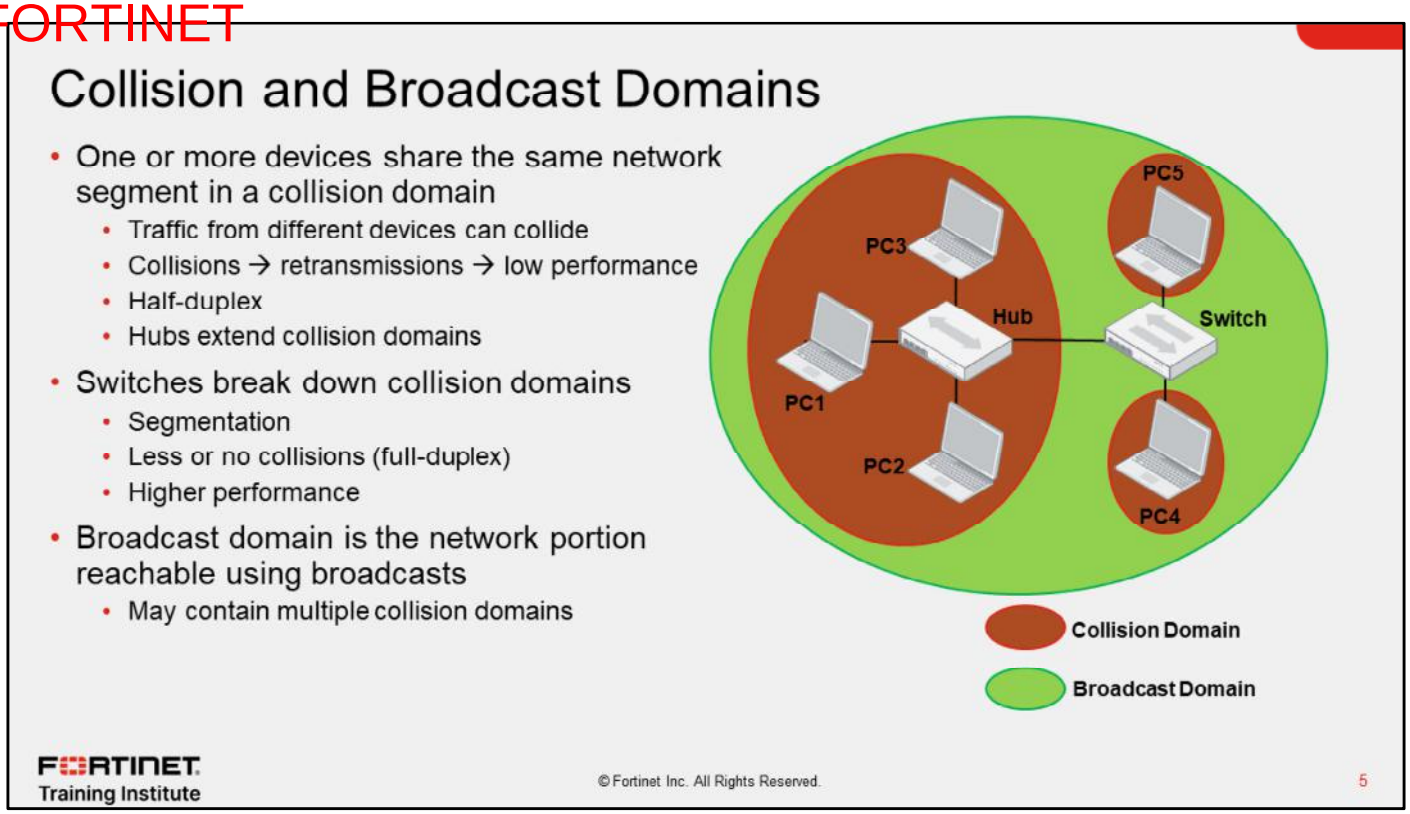
Switching is a key technology used to build computer networks. Switching enables wired devices that are connected to Ethernet switches to communicate with each other. To do this, switches forward Ethernet frames sent by connected devices based on the destination MAC address in the frame. A MAC address is a 48-bit unique identifier assigned to the network interface controller (NIC) of an Ethernet device. Because a device may have multiple NICs, a device may have multiple MAC addresses assigned (one for each NIC).

Ethernet switches operate at the data link layer (Layer 2) of the OSI model. Their forwarding decisions depend on the contents of their MAC address table, which is an internal data structure that switches maintain and that indicate the location of the different MAC addresses learned in the network.

Switches are usually found in LANs but can also be found in WANs. They provide high-performance connectivity by enabling network devices to transmit data at a very high speed with very low latency.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To better understand the benefits of using switches in your network, you should understand the concepts of collision and broadcast domains. A collision domain consists of one or more devices connecting to the same network segment. A network segment is a physical medium that is shared by one or more attached devices. Because devices in a collision domain share the same network segment, simultaneous data transmissions by multiple devices can collide with one another.

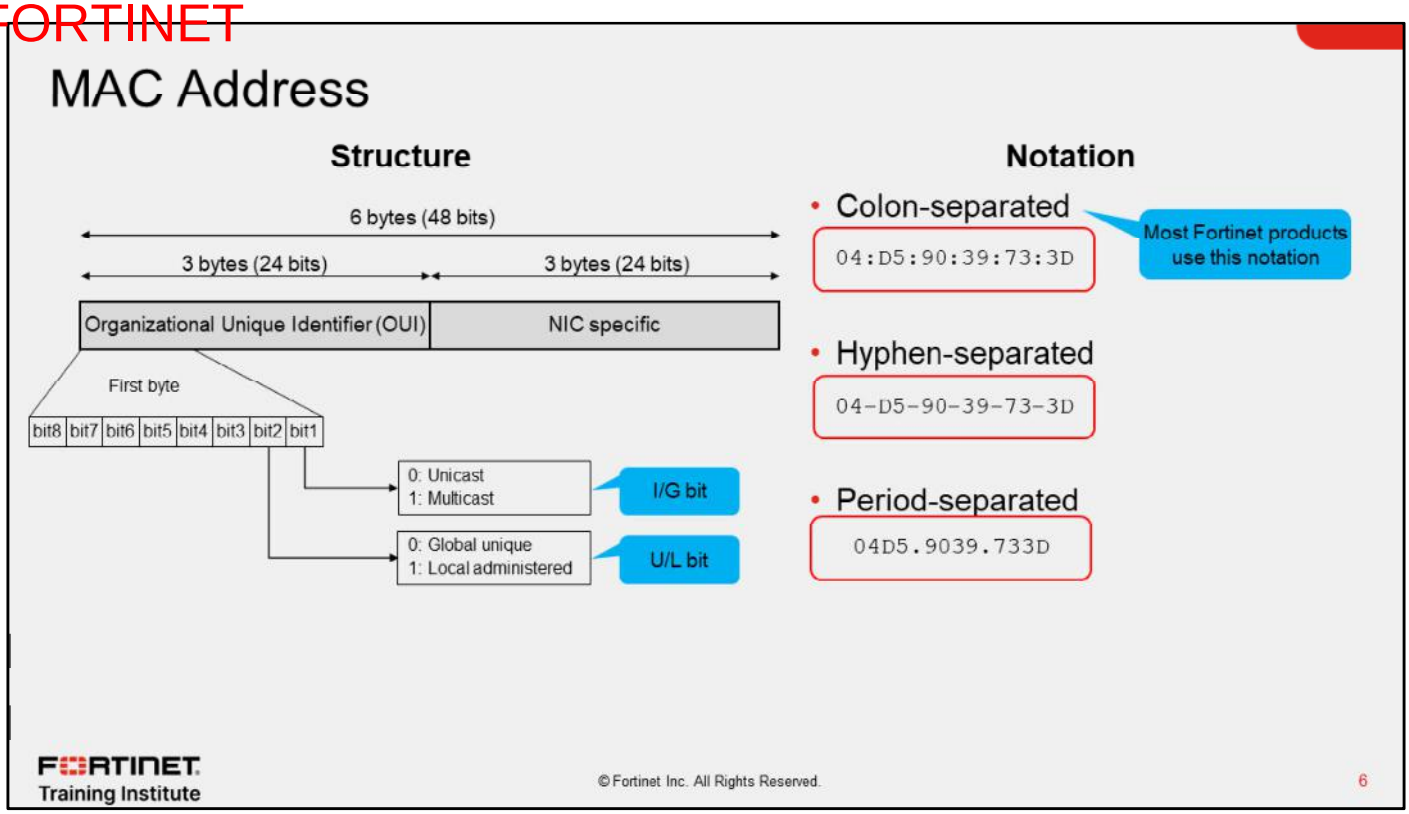
In modern networks, which use switches, you can think of a network segment as the physical connection between two devices—the most common example is the network cable connecting your computer to a switch. However, before switches existed, networks were deployed using hubs. Unlike a switch, a hub does not forward traffic based on Layer 2 information. Instead, when a hub receives a frame on any of its ports, it broadcasts the same frame to all other ports, regardless of the destination MAC address, and then lets the receiving devices decide whether to discard the frame or not. This behavior results in the network segment expanding into a larger collision domain, and therefore, in a higher chance of collisions occurring.

When switches were introduced, collisions were reduced or eliminated completely because of segmentation, which enables switches to break collision domains into smaller ones. Also, if a full-duplex connection is used between devices, collisions are no longer possible because devices now have dedicated channels to transmit and receive data in the network.

Broadcast domains refer to the logical portion of the network that can be reached using Layer 2 broadcasts. Although segmentation enables unicast frames to be forwarded to their intended targets only, all devices in a broadcast domain can still be reached using broadcasts. In the example shown on this slide, PCs 1 to 3 are in the same collision domain because they are connected to a hub, but PCs 4 and 5 are in separate collision domains because they are connected to a switch. In addition, all PCs in the diagram belong to the same broadcast domain.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



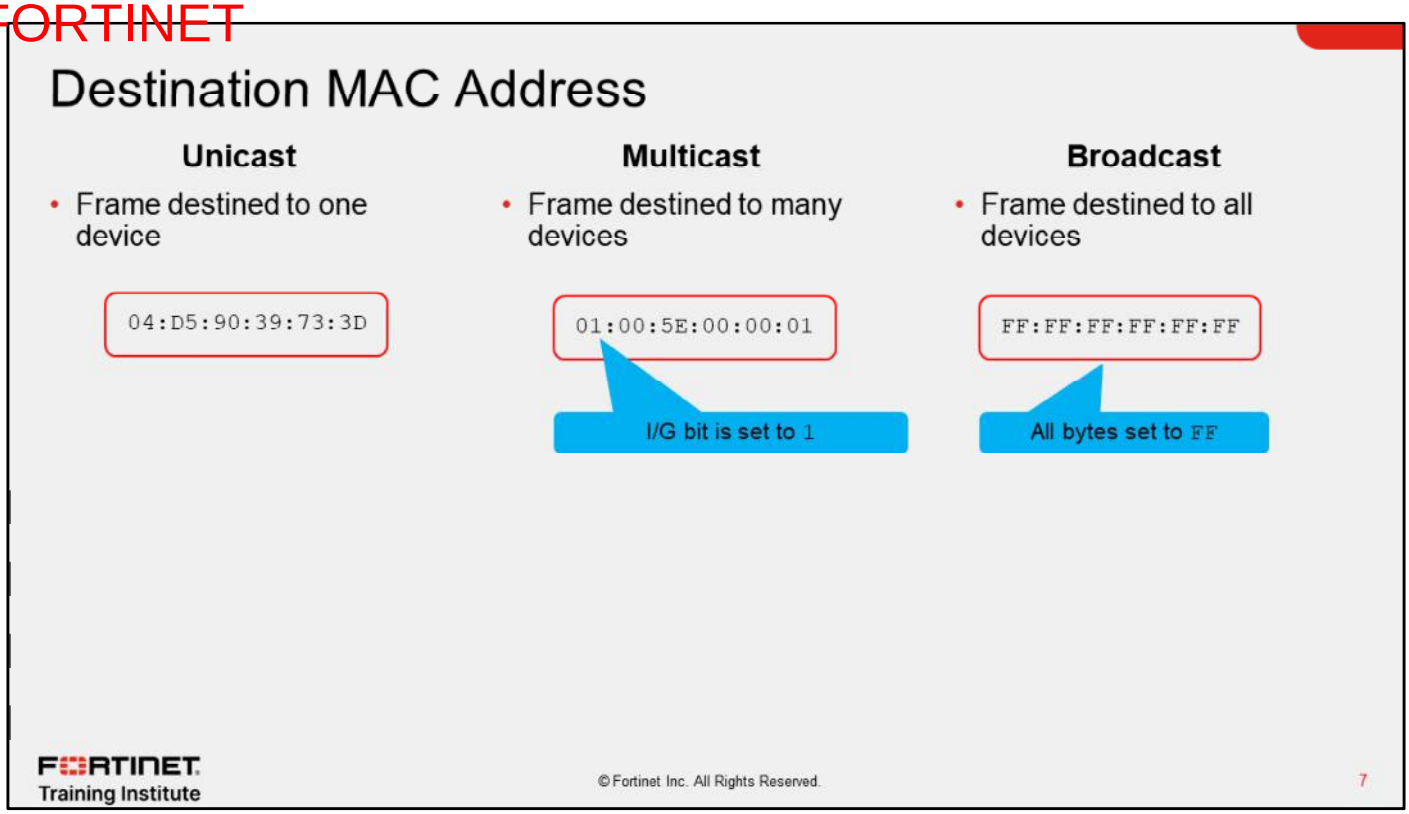
Ethernet switching uses MAC addresses to determine the source and destination of a frame. A MAC address is a 48-bit (or 6-byte) unique identifier assigned to the NIC that connects a device to the network. Although MAC addresses are assigned by NIC vendors and burned into hardware, users and applications can override that physical address with one that they choose. Overriding a physical MAC address is not common. However, sometimes you must manually set a different MAC address on a device NIC for it to work. A common case is when you need to set the same MAC address of a faulty device on the replacement because the adjacent device accepts a specific MAC address.

The MAC address structure can be divided into two 3-byte halves. The first half (from left to right) contains the organizational unique identifier (OUI), which identifies the NIC manufacturer. For example, two OUIs used by Fortinet are `04:D5:90` and `00:09:0F`. The least significant bit in the first byte of the OUI is called the individual/group (I/G) bit, and determines whether the address is unicast or multicast. The second least significant bit is called the universal/local (U/L) bit, and indicates if the address has been globally or locally administered. In most cases, both bits are set to `0`. However, if the Ethernet frame is for a multicast application, the I/L bit should be `1`. In addition, if the MAC address was locally configured by the administrator, the I/G bit should also be set to `1`. The last 3 bytes of a MAC address indicate the number specific to the device, which is known as the NIC specific.

This slide shows the three types of notations used for MAC addresses. Although most Fortinet products use the colon-separated notation, other options can be the hyphen and period-separated notations. The adoption of a particular notation varies among vendors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



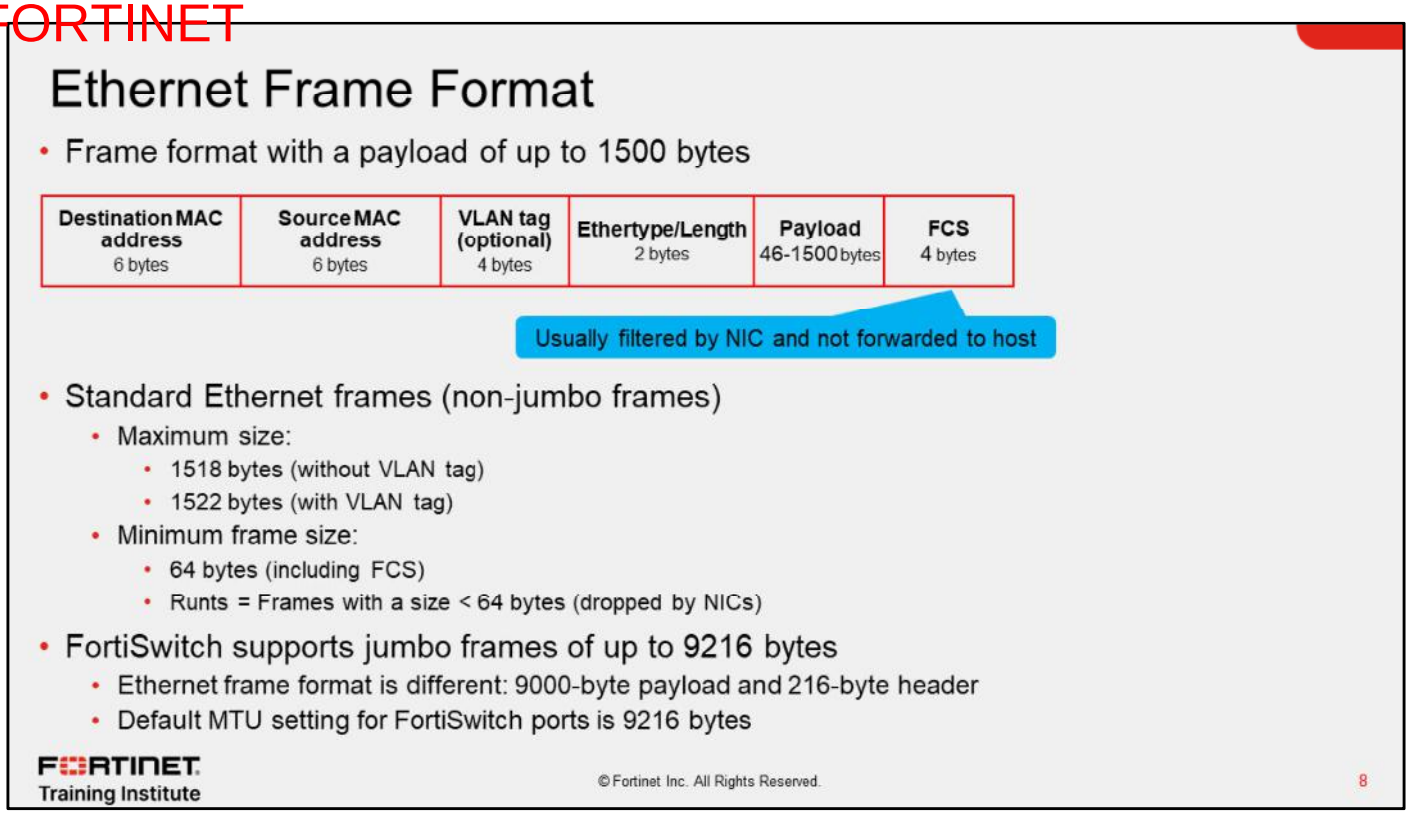
Like destination IP addresses in a packet, the destination MAC address in a frame depends on the type of transmission required by the network application, which can be unicast, multicast, or broadcast.

In unicast, the data is meant to be delivered to one receiver only. In multicast, the data is expected to be received by a group of devices that belong to a multicast group. In broadcast, all devices in the broadcast domain receive a copy of the frame.

In multicast, the I/G bit of the destination MAC address is always set to `1`. The sample multicast MAC address shown in the slide is for an Internet Group Management Protocol (IGMP) packet and has the I/G bit set to `1`. In broadcast, all bytes on the destination MAC address are set to `FF`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the format of an Ethernet frame with a payload of up to 1500 bytes.

- Destination MAC address: Indicates the MAC address of the destination.
- Source MAC address: Indicates the MAC address of the sender.
- VLAN tag: An optional tag that is added by devices to indicate the VLAN ID associated with a frame.
- Ethertype/Length: Can be used to either indicate the type of payload carried by the frame or its length. Most of the time, it's used to indicate the payload type. IPv4 and IPv6 packets are classified as Ethertypes `0800` and `86DD`, respectively.
- Payload: Carries the data being transported over Ethernet. In many cases, the payload is an IP packet.
- Frame check sequence (FCS): Used for detecting corrupted data.

The FCS is usually checked on the NIC level and removed from the frame by the NIC before the frame is forwarded to the host for further processing. This is the reason why Wireshark doesn't display the FCS in the Ethernet header, and more importantly, why Ethernet frames are usually considered to have a maximum size of 1518 bytes (without VLAN tag) or 1522 bytes (with VLAN tag), unless jumbo frames are used. Note that the minimum frame size is 64 bytes (including FCS). Frames smaller than 64 bytes are called runts and should be discarded by NICs.

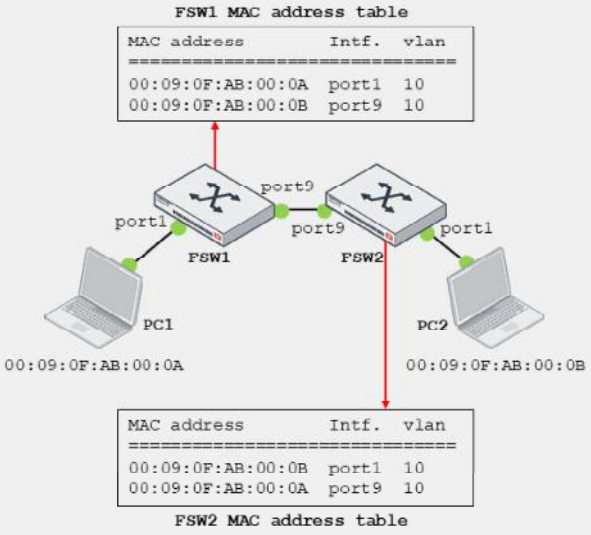
Jumbo frames can carry a payload of up to 9000 bytes. FortiSwitch uses a 216-byte header for jumbo frames, which results in a maximum frame size of 9216 bytes. The maximum frame size on a port is also known as the maximum transmission unit (MTU). All ports in FortiSwitch are configured with an MTU of 9216 bytes by default, so jumbo frames are supported out of the box. Do not confuse the frame MTU with the IP MTU. The former refers to the Ethernet frame size and the latter to the IP packet size. When you adjust the MTU setting on a switch, it usually affects the frame size. When you adjust the MTU setting on a router or on any other Layer 3 device, it usually affects the IP packet size.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MAC Learning and Frame Forwarding

- MAC address table
  - Maintained by switches
  - Maps MAC addresses to interfaces and VLANs
  - MAC addresses are learned from ingress traffic
  - Most entries are dynamic (aging) but some are static
- Forwarding is based on destination MAC and MAC table contents
  - Switch forwards the frame to the port where the destination MAC was learned
  - If the MAC is not in the MAC table, the switch floods the frame to all ports except the ingress port



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Switches forward traffic based on the frame destination address and the contents of the MAC address table. A MAC address table is an internal data structure maintained by the switch and contains an entry for each MAC address learned on a port, including the interface and VLAN where the MAC address was learned.

The switch learns MAC addresses when processing incoming traffic. When the switch receives a frame, it looks at the source MAC address. If the switch does not have an entry for that MAC address in the MAC address table, the switch creates a new entry—a dynamic entry—and assigns an aging timer to it. Dynamic entries are removed from the MAC address table after their aging timer expires. The aging timer is usually five minutes, but it can vary among vendors. A MAC address table may also contain static entries. The static entries are either configured by the administrator or automatically created by the switch for internal interfaces that are used for processing system traffic, such as management.

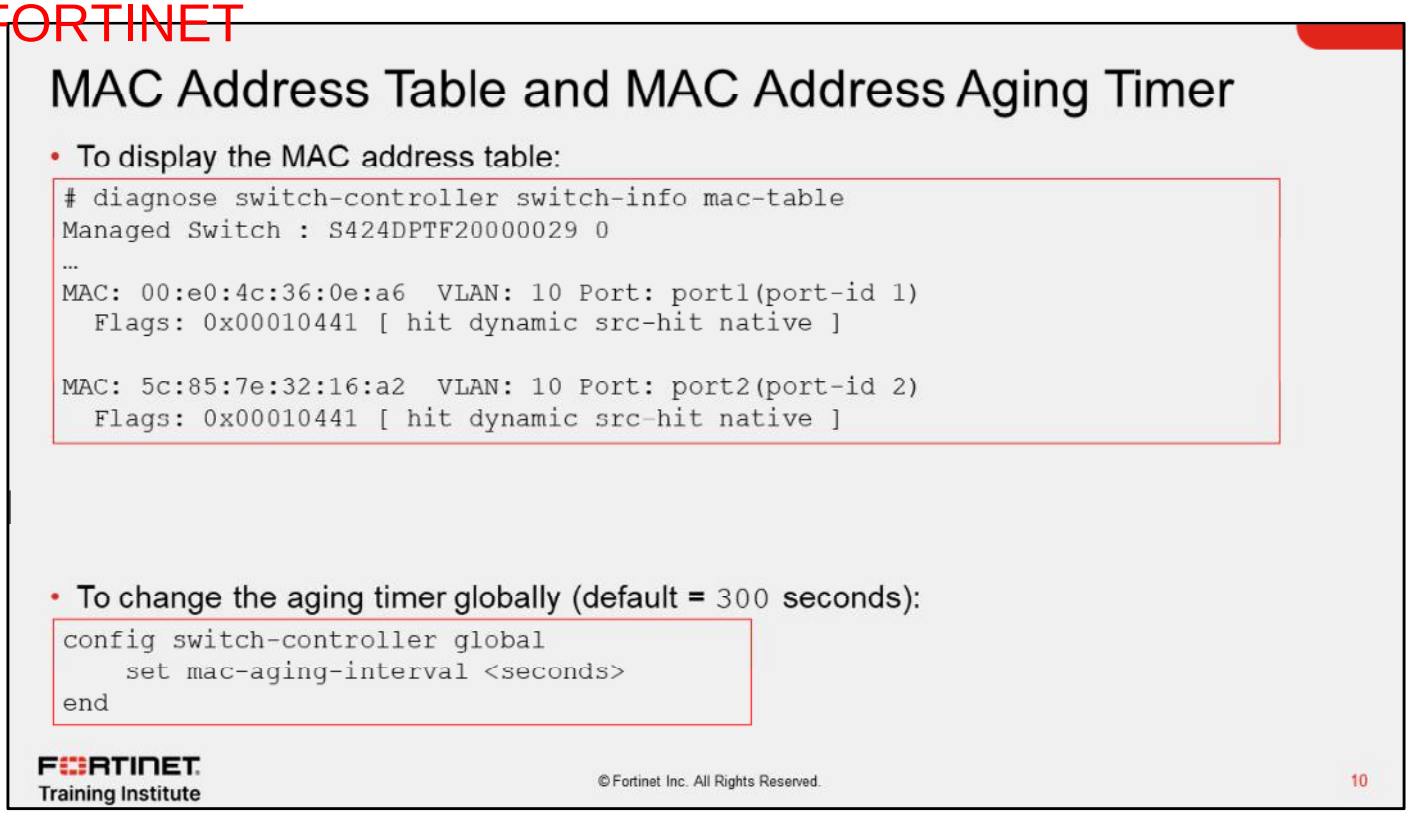
In the case where the switch finds a matching entry for the source MAC address, it updates that entry and resets the aging timer of that specific entry.

After the switch creates a new entry for the source MAC address or updates an existing one, it looks at the frame destination MAC address and looks for a match in the MAC address table. If there is a match, the switch forwards the frame to the interface associated with the entry. If there is no match, the switch floods the frame to all its ports except the port where the frame was received.

The example on this slide shows two switches—FSW1 and FSW2—and two computers assigned to VLAN 10—PC1 and PC2. The MAC address of PC1 is seen on port1 on FSW1 and port9 on FSW2. the MAC address of PC2 is seen on port1 on FSW2 and port9 on FSW1. When FSW1 receives a frame destined to the MAC address of PC2, it forwards the frame to port9. FSW2 then receives the frame on port9 and forwards it to port1, which is where PC2 is connected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The `diagnose switch-controller switch-info mac-table` command displays the FortiSwitch MAC address table.

The default aging timer for learned MAC addresses is 300 seconds (5 minutes). Usually, this value works well for most networks. However, if you want to adjust the timer globally, you can run the commands shown on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which address is used by Ethernet switches to forward frames?
   - ✓ A. Destination MAC address
   - B. Source MAC address

2. Which statement about collision domains and broadcast domains is true?
   - ✓ A. A broadcast domain may contain multiple collision domains.
   - B. Hubs break down collision domains.

3. Which portion of the MAC address identifies the NIC manufacturer?
   - A. NIC specific
   - ✓ B. OUI

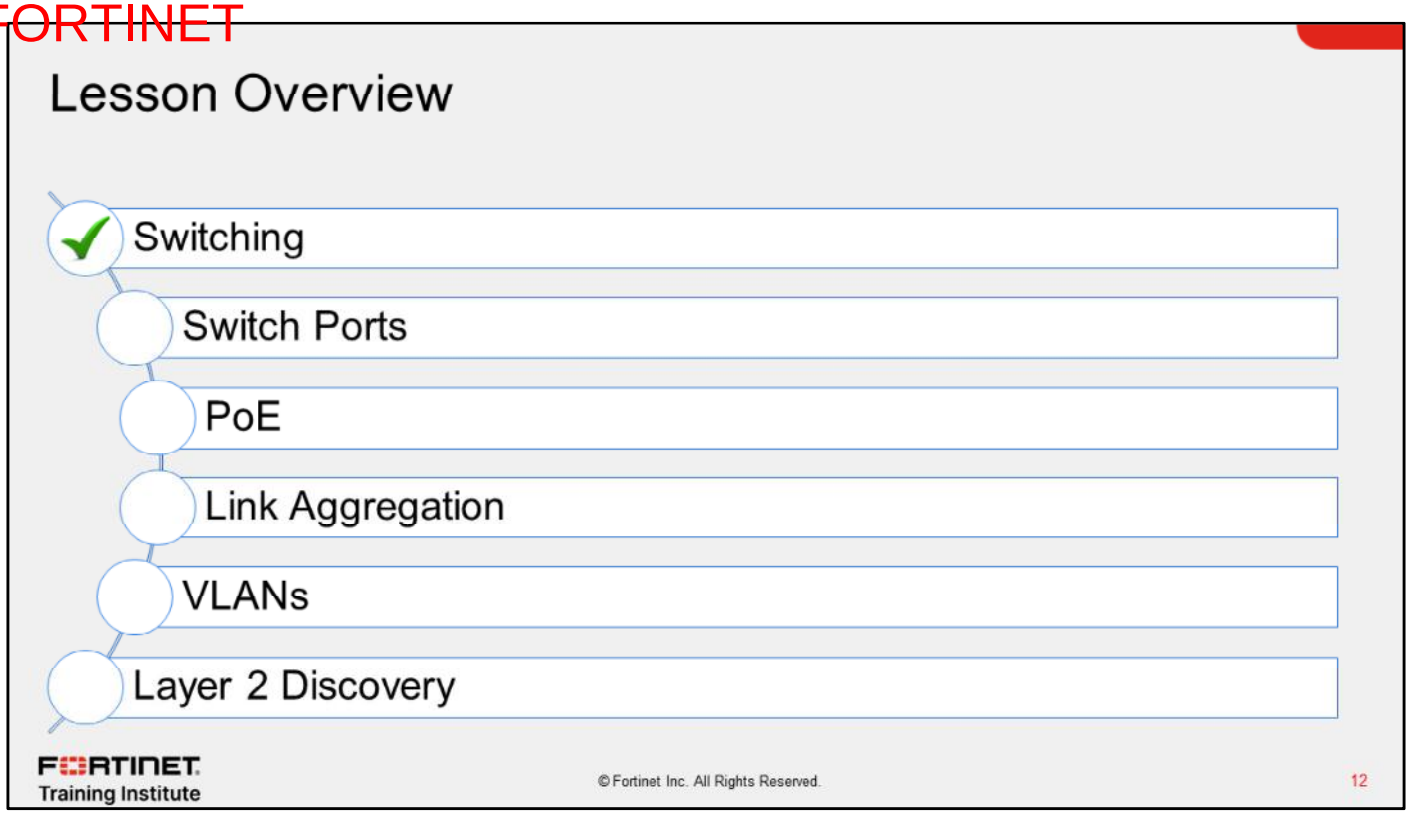
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

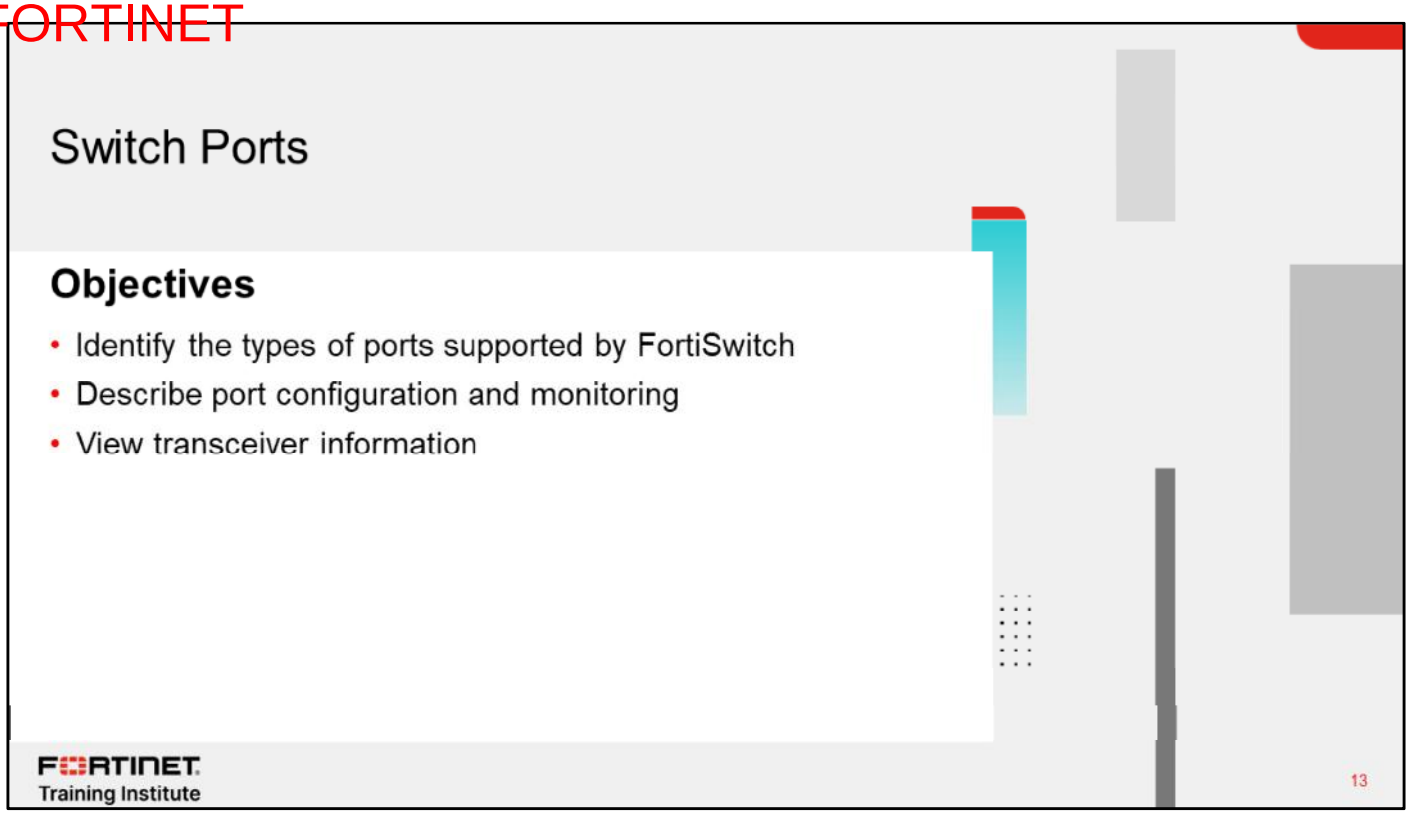


Good job! You now understand switching.

Now, you will learn about switch ports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

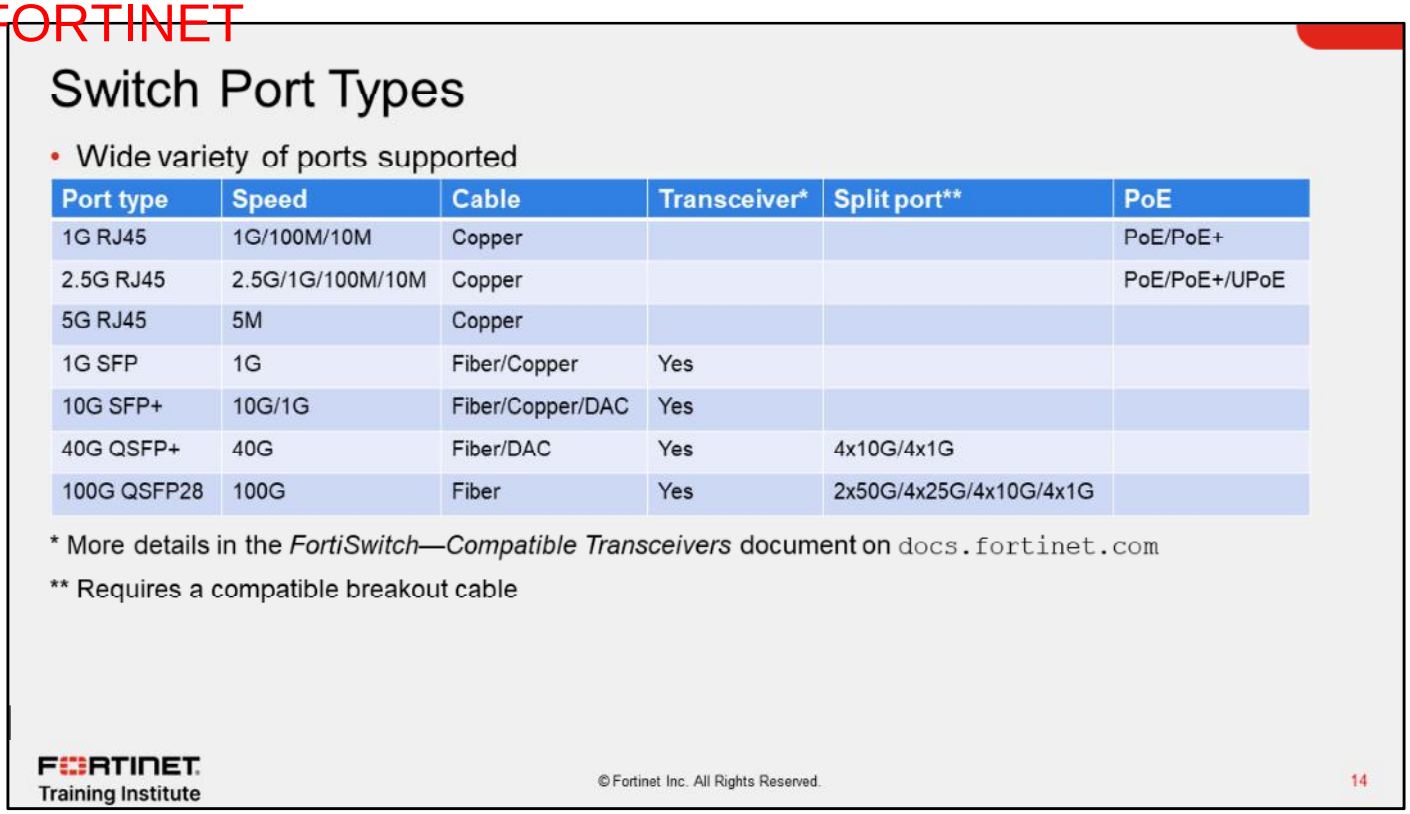


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in switch ports, you should be able to identify the ports required by your FortiSwitch stack deployment, as well as configure and monitor them on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiSwitch portfolio supports a wide variety of ports to meet different network connectivity requirements. The table on this slide shows the different port types, their supported speeds, and cable types. The table also indicates whether the port requires a transceiver, and if it supports split port and Power over Ethernet (PoE).

The supported port types are either RJ45 or a small form-factor pluggable (SFP) variant. RJ45 uses copper cable only, while SFP can use fiber, copper, or direct attach copper (DAC) cables. The main advantage of using an SFP-type transceiver is that you can use different cable options, which provides you with more flexibility to meet cost, distance, and performance requirements. For example, you can use fiber cabling if you need to extend your network to longer distances, or you can use DAC cables if you want to reduce costs without affecting performance. A DAC cable is a twinax copper cable that connects directly to the switch port and network device. A DAC cable is more cost-effective because is factory terminated with a transceiver and therefore, there is no need to get separate transceivers to plug the cable in.

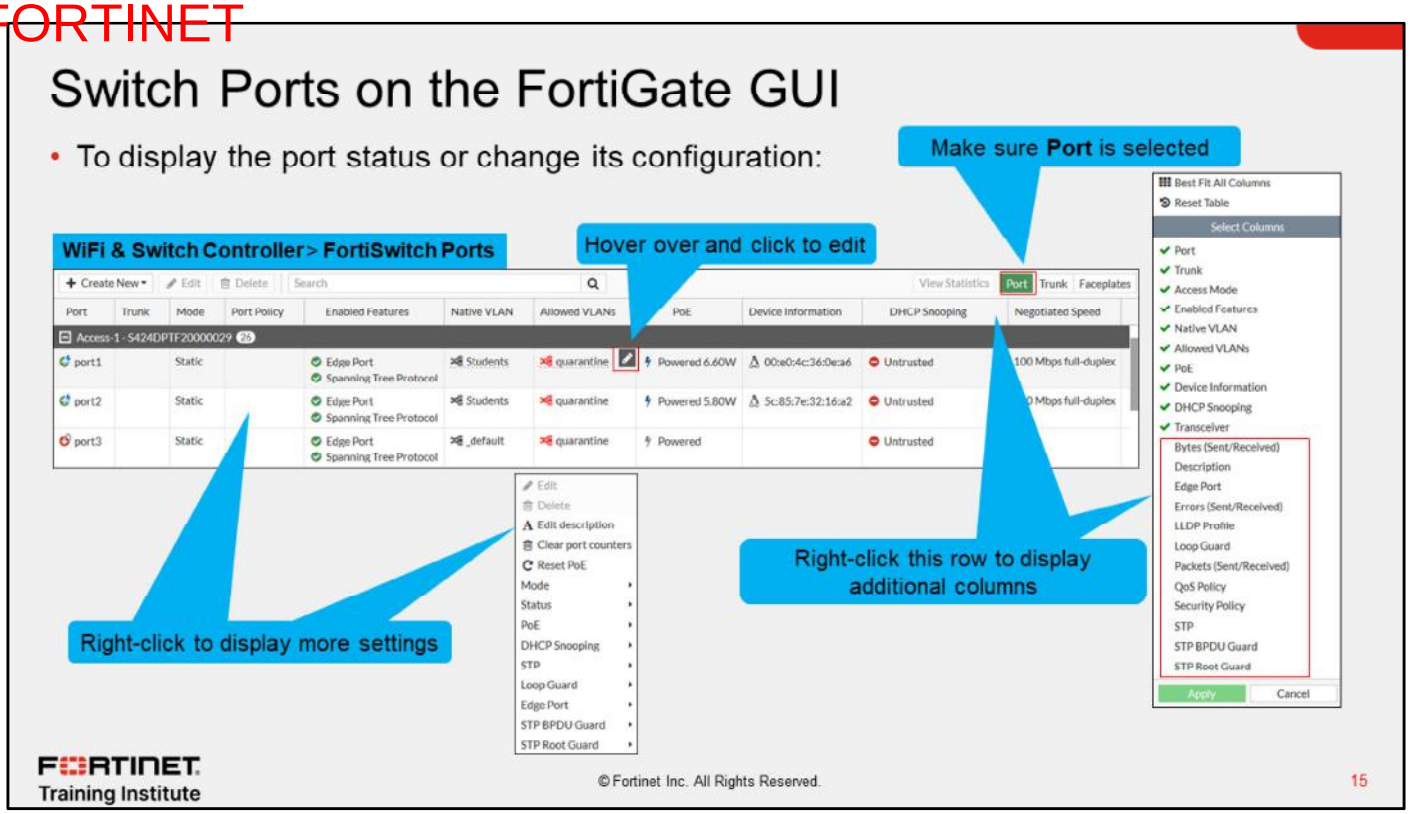
FortiSwitch supports the following types of SFP:

- SFP: The first SFP version. It supports a fixed speed of 1G. You can use fiber or copper cables.
- SFP+: An improvement to SFP that enables data rates of up to 10G. It's backward compatible with SFP.
- Quad SFP+ (QSFP+): An evolution of SFP+. It carries four 10G channels to provide a 40G connection. The port can be split into four individual 10G ports (breakout cable needed).
- QSFP28: Offers the highest performance: 100G. The port can be split into 2x50G, 4x25G, or 4x10G (breakout cable needed).

You will learn more about the split port feature in another lesson. For more information about compatible transceivers for each FortiSwitch model, refer to the *FortiSwitch—Compatible Transceivers* document on `docs.fortinet.com`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **FortiSwitch Ports** page displays all the switch ports available for each managed switch. The page also shows information about switch trunks and faceplates, so make sure you select the **Port** tab to display the information for switch ports.

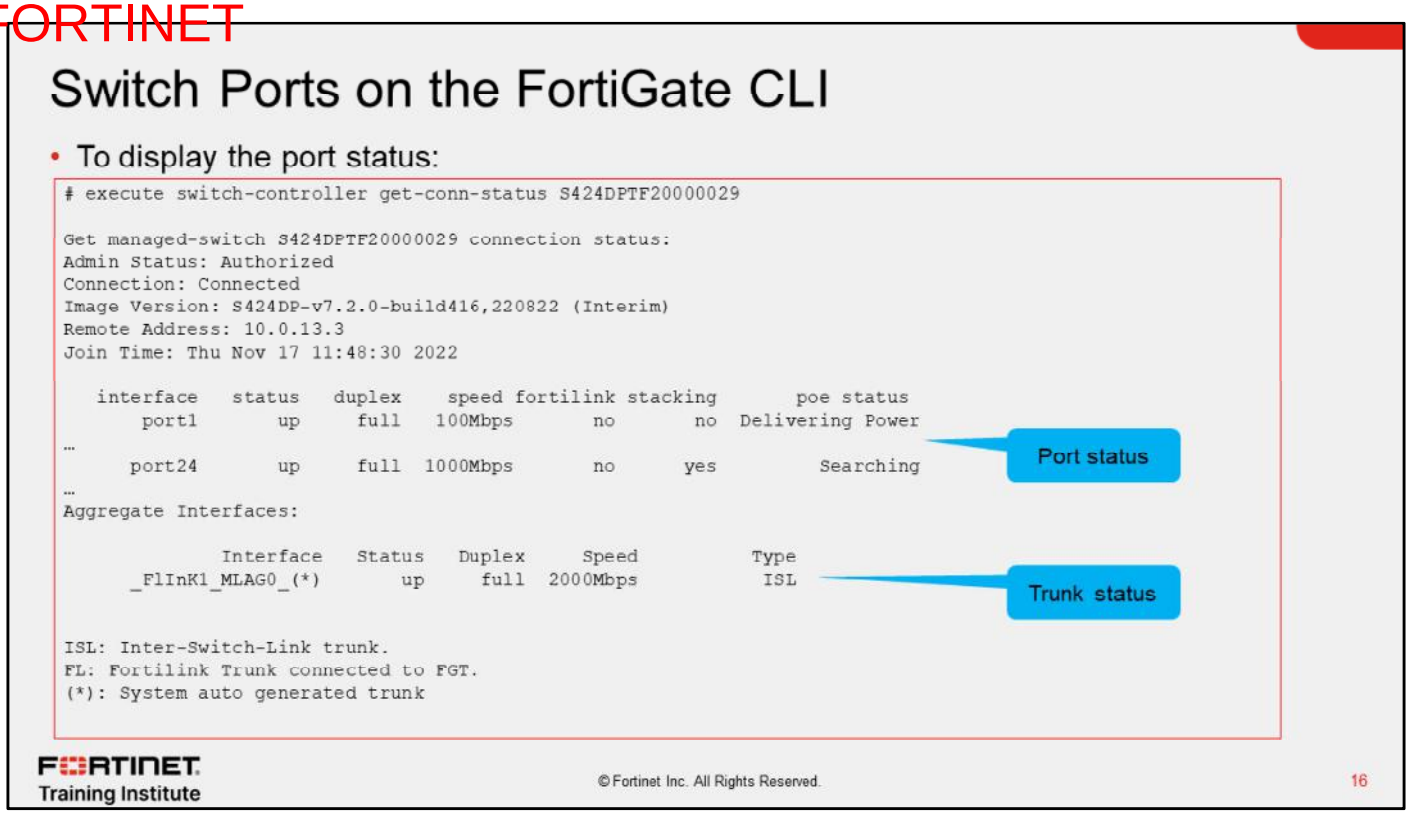
In addition to viewing the status of each port, you can also view or edit the port configuration. To edit the settings on a port, hover over the setting in the column you want to edit. The settings in some columns show status information only and cannot be edited. Settings that can be edited show a pencil icon when you hover over them. You can then click the pencil icon to change the setting. If the setting you are looking for is not shown, right-click the top cell of any column to display a context menu containing the additional columns you can add to the page.

You can also right-click a port to display a context menu with some actions you can perform on the port and some port settings that you can change.

You will learn more about the different port settings in multiple lessons throughout this course.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

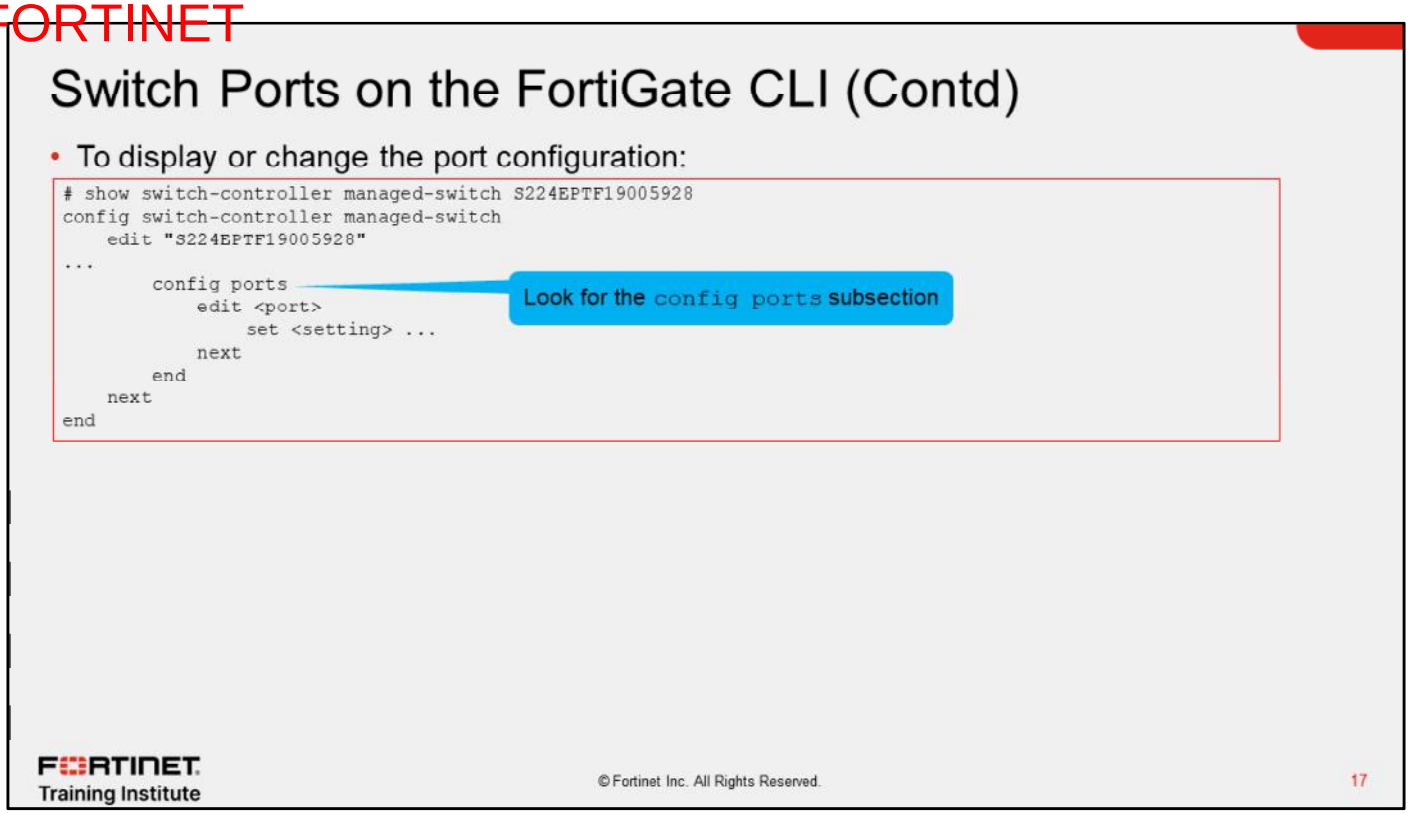


You can get the status of all switch ports on the FortiGate CLI by running the `execute switch-controller get-conn-status` command. Make sure you add the switch ID at the end of the command—otherwise, the port information won't be included.

The output also includes the trunk information. You will learn more about trunks in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

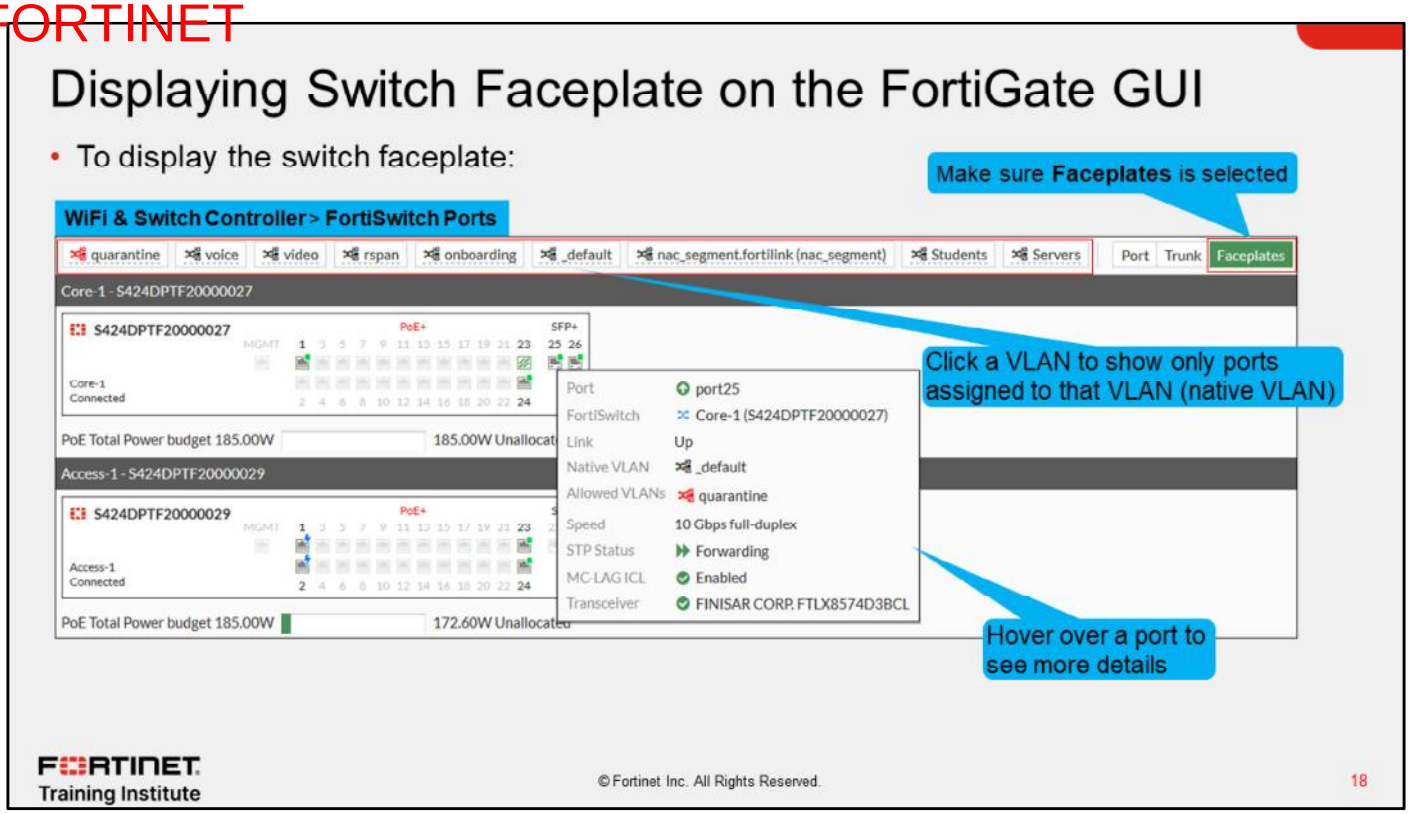
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The port configuration of a managed switch has a separate sub-section under `config switch-controller managed-switch`. Use the `show` command to display the port configuration or navigate to the `config ports` subsection to edit one or more settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



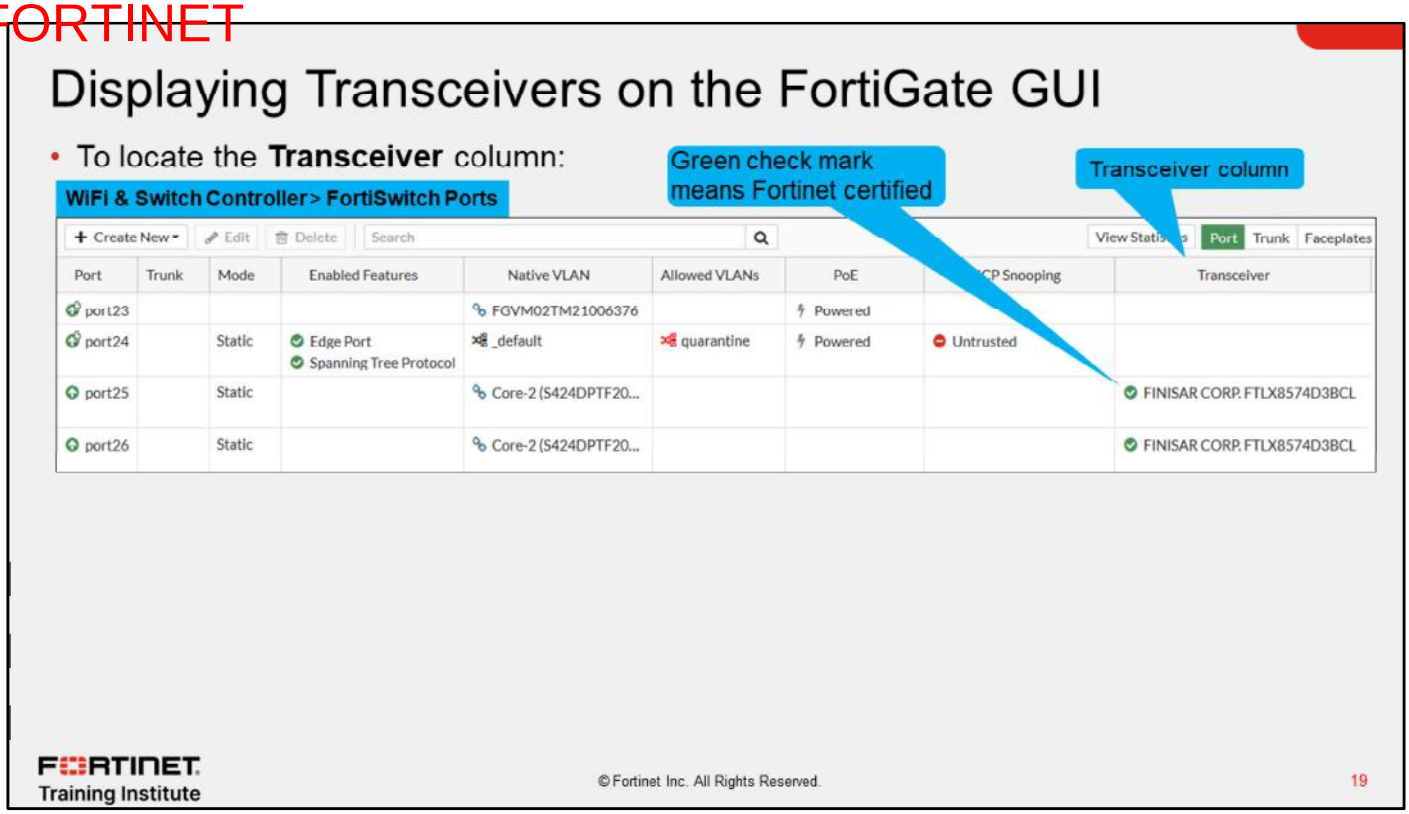
The FortiLink discovery frames broadcast by FortiSwitch during switch discovery contains the list of ports on the switch and their type. FortiOS uses this information to build the faceplate for the switch, which you can see on the **Faceplates** tab on the **FortiSwitch Ports** page.

At the top of the page, you can see a list of FortiSwitch VLANs created on FortiGate. When you click one, the faceplate highlights the ports that are assigned to that native VLAN.

You can hover over a port to see more information about it, such as the link status, FortiSwitch device it belongs to, assigned VLANs, PoE, and Spanning Tree Protocol (STP) status. You will learn more about PoE in this lesson, and about STP in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can view transceiver basic information on the **FortiSwitch Ports** page. Locate the **Transceiver** column and hover over the transceiver you want information about. The GUI displays basic information, such as the transceiver type, vendor name, and part number.

If the transceiver is certified by Fortinet, a green check mark appears beside it. If you use a transceiver that is not certified by Fortinet, a yellow warning icon appears instead. Fortinet recommends using certified transceivers because they have been fully tested and therefore, guaranteed to work under normal operating conditions. For more information about compatible transceivers for each FortiSwitch model, see the *FortiSwitch—Compatible Transceivers* document on `docs.fortinet.com`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying Transceivers on the FortiGate CLI

- To get summarized transceiver information:

```
 # diagnose switch-controller switch-info modules summary S424DPTF20000051 port25
Vdom: root

S424DPTF20000051:

  Portname   State    Type      DMI  Transceiver    RX  Vendor           Part Number      Serial Number
  _________ _______  _______   ___  ___________    __ _______________ ________________ _____________

  port25     INSERT   SFP/SFP+  Y    10G-Base-SR    OK  FINISAR CORP.    FTLX8574D3BCL    A4JABMT
```

FORTINET Training Institute

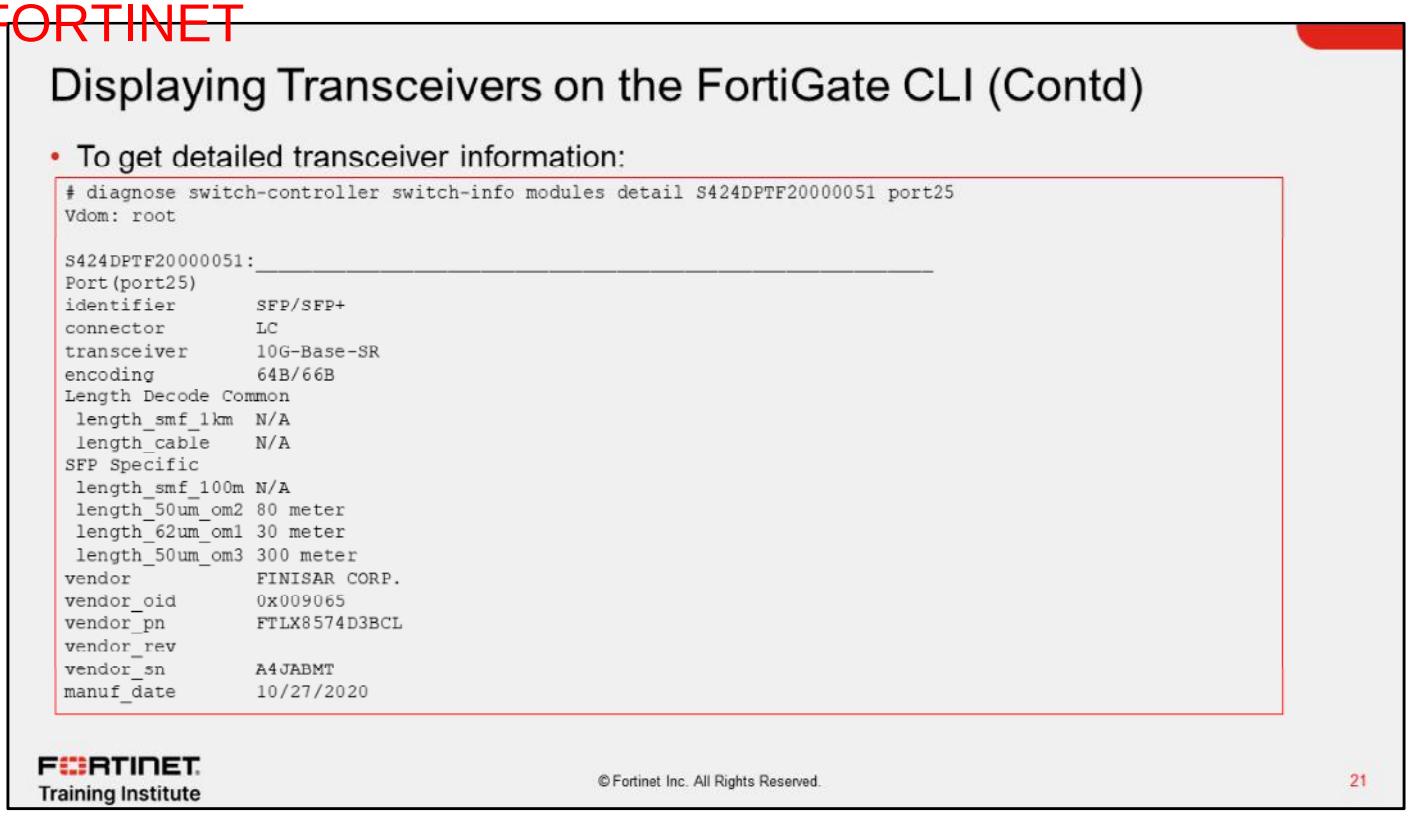
© Fortinet Inc. All Rights Reserved.

20

You can also see basic transceiver information on the FortiGate CLI by running the command shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you want to see detailed transceiver information, you must use the CLI command shown on this slide. The additional information displayed includes the connector type, encoding method, and the supported fiber cable types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about the 100G QSFP28 port is true?

✓A. It requires a compatible transceiver.

B. It does not support split port.

2. Which FortiOS command can be used to display transceiver information?

A. `execute switch-controller get-conn-status <switch-id>`

✓B. `diagnose switch-controller switch-info modules summary`

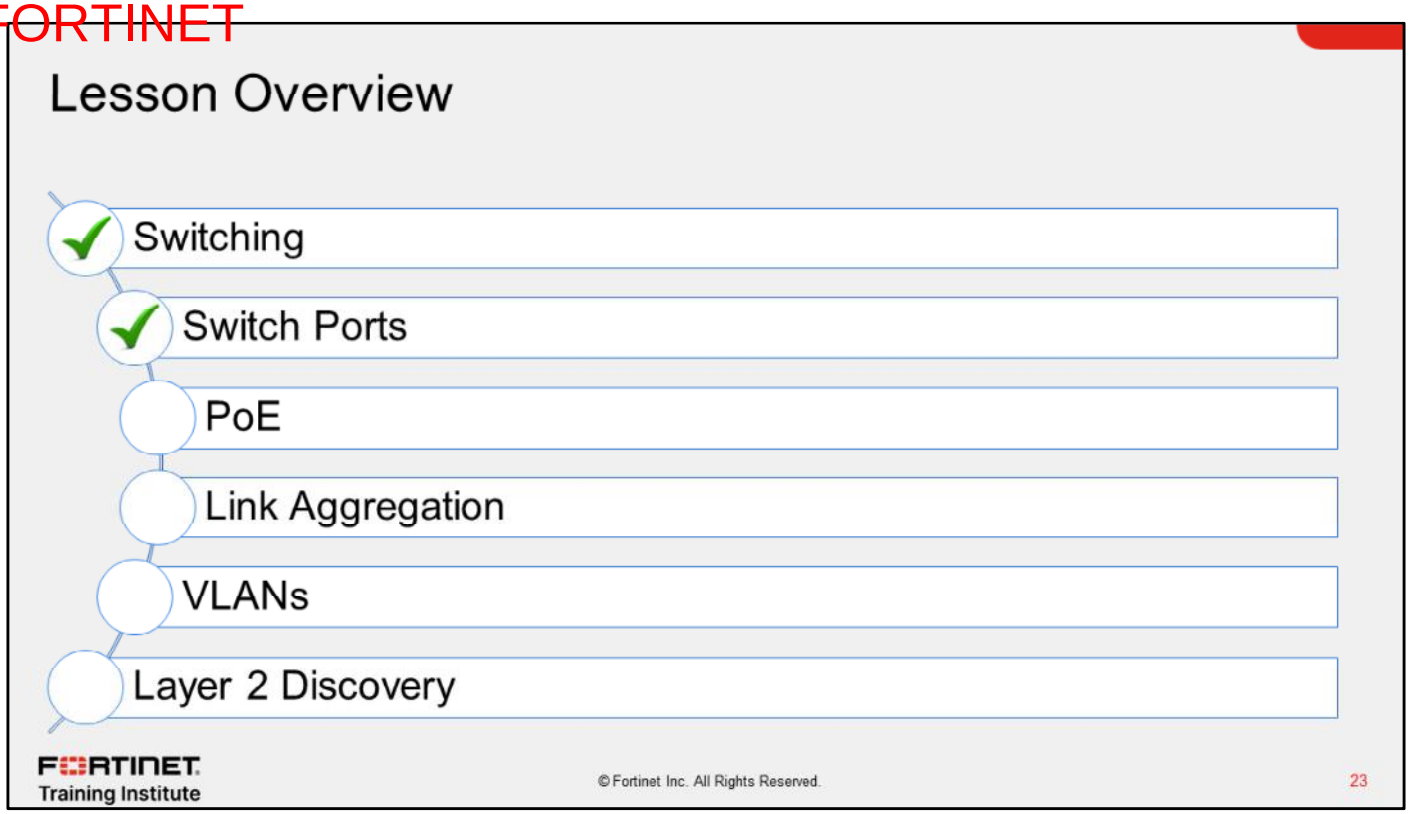
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

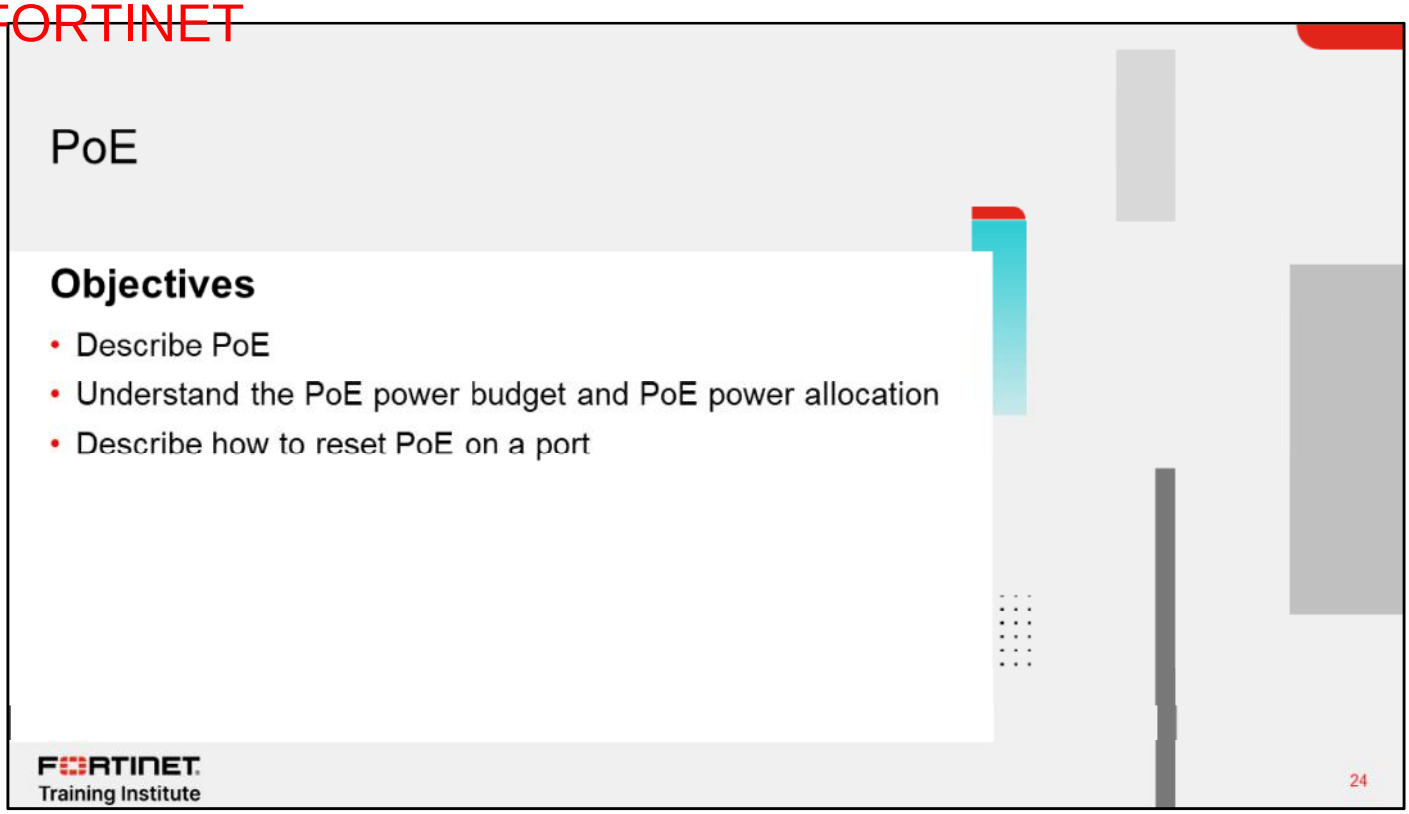


Good job! You now understand switch ports.

Now, you will learn about power over Ethernet (PoE).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in power over Ethernet (PoE), you should be able to understand the benefits of PoE, how much power a PoE-capable FortiSwitch can deliver, and how FortiSwitch prioritizes power allocation to devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

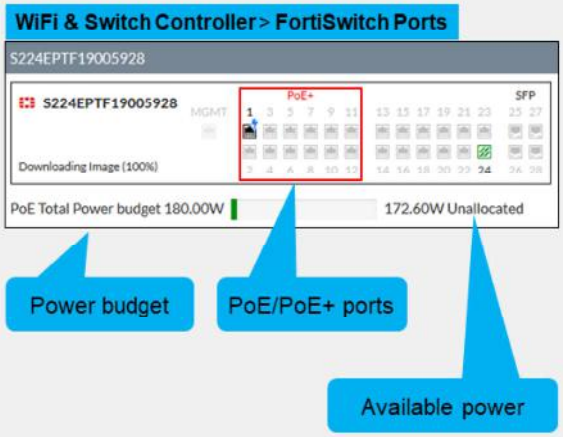
What Is PoE?

- Single cable to provide power and data to PDs
  - Less cabling on PDs and easier installations
  - Enables remote power cycling of PDs
- PoE standards:

Property	PoE	PoE+	UPoE***
Max. power on port*	15.4 W	30 W	60 W
Power on PD**	12.95 W	25.50 W	51 W
IEEE standard	802.3af	802.3at	802.3bt type 3
Min. cable type	Cat. 3	Cat. 5	Cat. 5

* Used to calculate current total allocated power
** Lowest guaranteed power on PD when port delivers maximum power
*** Only available on FortiSwitch M426E-FPOE

- PoE standards are backward compatible



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

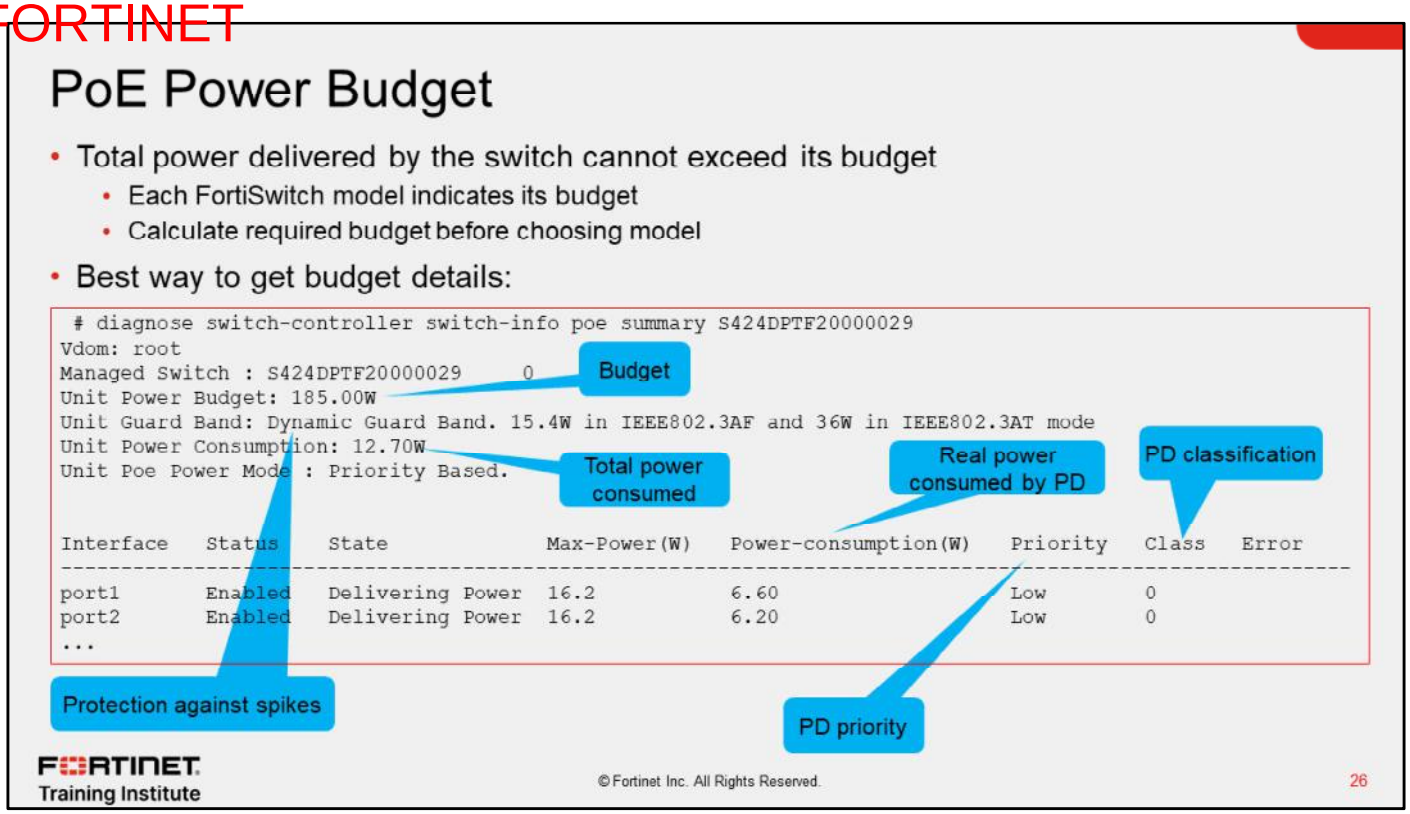
PoE enables switches to transmit electric power to endpoints through twisted pair Ethernet cables. The goal is to use the same Ethernet cable to provide both power and data and therefore reduce the amount of cabling required for powered devices (PDs). Common examples of PDs include VoIP phones, wireless access points, and IP cameras. Another benefit of using PoE is that it simplifies PD installation because less cabling is required. Using PoE also enables you to install PDs in otherwise impractical places, such as ceilings. Also, PoE enables you to power cycle the PDs from the switch, without requiring on-site assistance or a separate remote power management system.

The table on this slide describes the most widely used PoE standards, each of them supporting different power capacities. The first PoE version can deliver up to 15.4 W on a port. Each subsequent newer version of the standard doubles the maximum power of the previous one, while still being backward compatible. Note that some of the power delivered to PDs is dissipated on the cable. For this reason, a minimum guaranteed power on the PD, when the port delivers the maximum power, is also indicated.

The FortiSwitch secure access and rugged series support PoE and PoE+ with some models supporting UPoE. The datasheet for each switch indicates its PoE-capable ports and its PoE power budget. You can also see the PoE power budget information on the **Faceplates** tab on the **FortiSwitch Ports** page. Note that the total amount of power delivered by a switch cannot exceed its budget.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



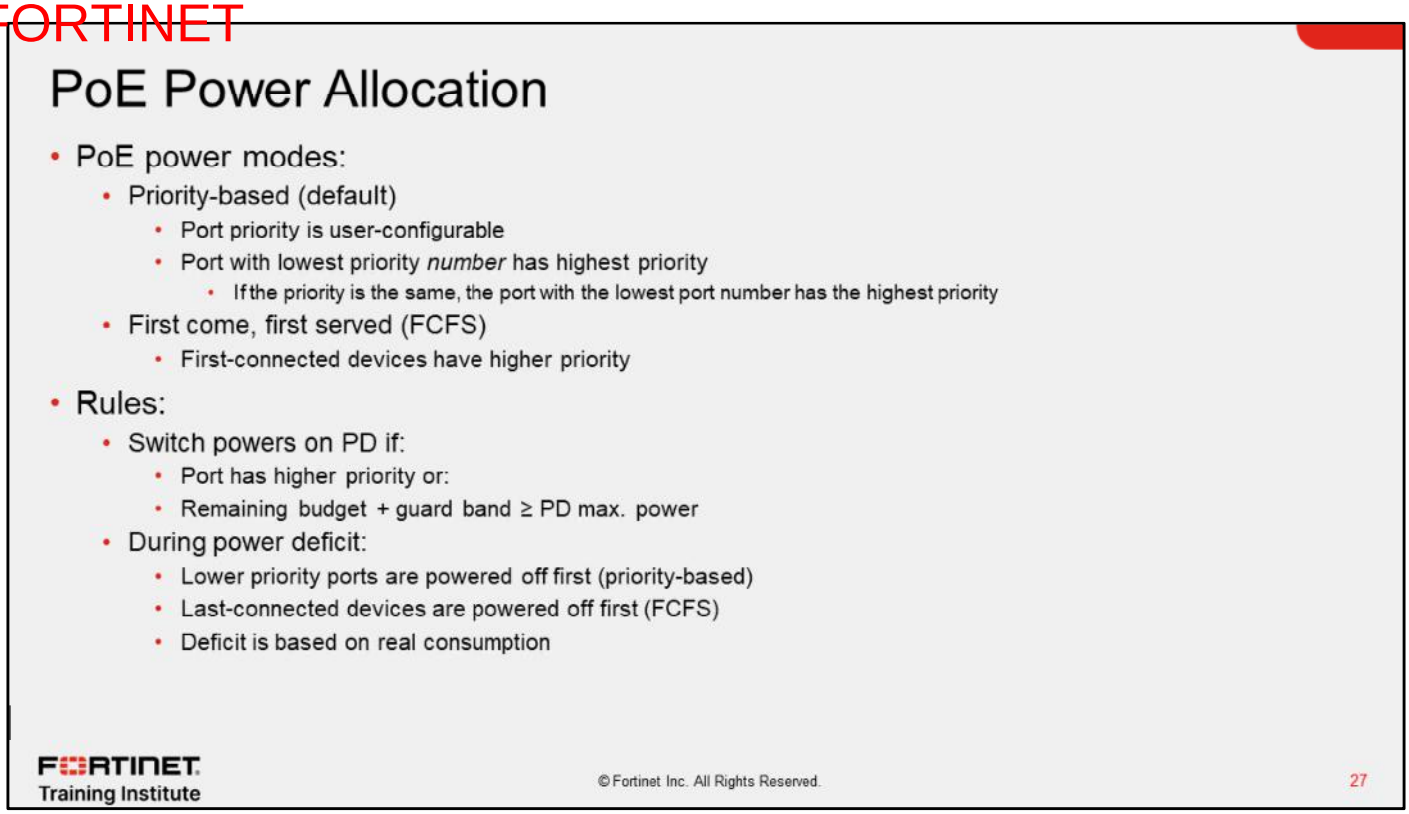
The total amount of power delivered by all PoE ports on a switch cannot exceed its budget. In some cases, this may result in the switch not being able to deliver power on some ports. For example, a FortiSwitch 224E-POE has 12 PoE/PoE+ ports and a budget of 180 W. If you connect 12 PoE devices to the switch, the switch can deliver power to all 12 devices even if they consume the maximum power available on the port. However, if the devices are PoE+, and require the maximum available power on the port, the switch is capable of powering only half of the devices.

The best way to view the PoE power budget details is by using the CLI command shown on this slide. The output shows the PoE power budget and the real amount of power used by the switch. The output also includes PD consumption details on each port. PDs are assigned a class based on the amount of power they require. The switch gets the class from the PD after the PD connects to the port. Although each class is assigned a maximum power on the port, the real amount of power consumed by a PD can be much lower.

Finally, the PoE guard band reserves an additional amount of power that is used by the switch for dealing with sudden spikes in PoE consumption.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you connect a PD to FortiSwitch, the switch must determine whether it can power the PD or not. The way the switch makes this decision depends on the PoE power mode, port priority, power consumption status, and the power required by the PD.

When there is a power deficit, the switch supports two modes for determining which devices have priority over others for power delivery: priority-based and first come, first serve (FCFS). The former is the default mode, and instructs the switch to cut the power to PDs with a lower priority in favor of those with a higher priority. The administrator can configure the port priority. If there are two or more ports with the same priority, the port number is used as a tiebreaker—the port with the lowest port number has the highest priority. In FCFS mode, the switch prioritizes PDs that connected first over those connected last.

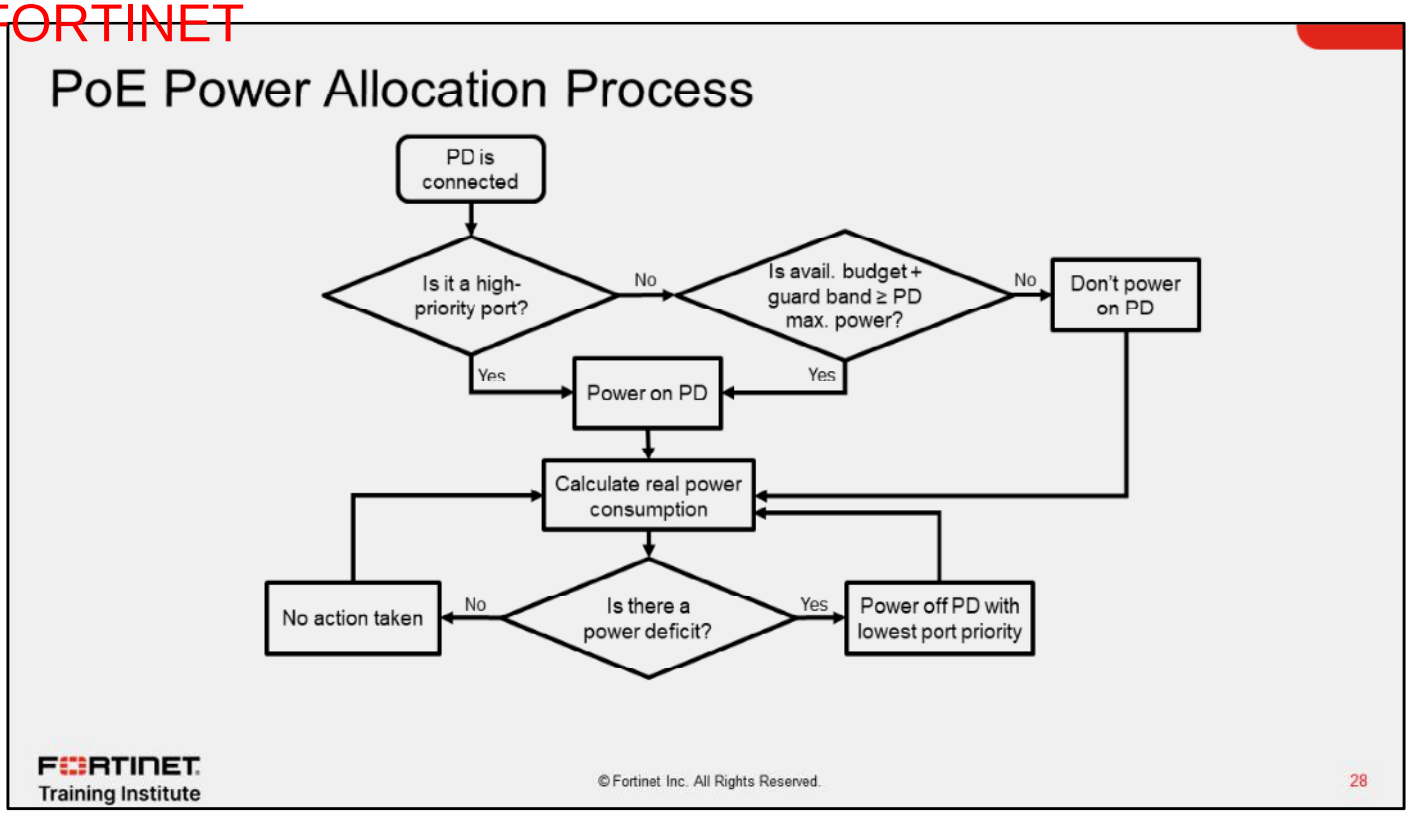
After FortiSwitch determines whether to power on a PD, the switch continues monitoring its total real power consumption. When a power deficit occurs, the switch takes one of the following actions based on the power mode configured:

- If the mode is priority-based, devices connected to ports with a lower priority are powered off first.
- If the mode is FCFS, devices that connected last are powered off first.

Note that the power deficit is calculated based on real power consumption.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The flow chart on this slide describes the PoE power allocation process that occurs when you connect a PD to FortiSwitch. The flow chart applies to both priority-based and FCFS modes.

First, FortiSwitch compares the priority of the port connected to the PD with the priority of other active PoE ports, and then proceeds as follows:

- If the port has a higher priority, FortiSwitch powers on the PD.
- If the port has a lower priority, FortiSwitch checks if the amount of power available in the budget plus the guard band is higher than or equal to the PD maximum power. If so, FortiSwitch powers on the PD. If not, it does not power on the PD.

Note that if in FCFS mode, the port is always considered low priority after you connect the PD—it's the last connected port. For this reason, in FCFS mode, FortiSwitch powers on the PD only if its consumption is lower than or equal to the available budget plus the guard band.

After FortiSwitch determines whether to power on a PD, it continuously monitors the total real power consumption on the switch. When there is a power deficit, FortiSwitch powers off the PD connected to the port with the lowest priority. In FCFS mode, the lowest priority port is the last connected port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Resetting PoE on a Port

- Disabling a port does *not* stop power delivery
- To reset PoE on a port:
  - Use the context menu on the **FortiSwitch Ports** page:



  - Or use the CLI command:

```
# execute switch-controller switch-action poe reset S224EPTF19005928 port1
Toggling power on port1.........
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

Administratively disabling a port does *not* stop power delivery on that port. Instead, you must reset PoE on the port using the FortiGate GUI or CLI.

On the FortiGate GUI, browse to the **FortiSwitch Ports** page, right-click the port you want to reset PoE on, and then select the **Reset PoE** action in the context menu.

On the FortiGate CLI, run the command shown on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about PoE support in FortiSwitch is true?
   A. The FortiSwitch data center series supports PoE.
   ✓ B. PoE standards are backward compatible.

2. When using priority-based PoE mode and a power deficit occurs, which port is powered off if the priority for multiple ports is the same?
   A. The lowest-numbered port
   ✓ B. The highest-numbered port

3. Which statement about the PoE power budget is true?
   ✓ A. It varies among PoE-capable FortiSwitch models.
   B. There is always enough power to supply all PDs connected to the switch.

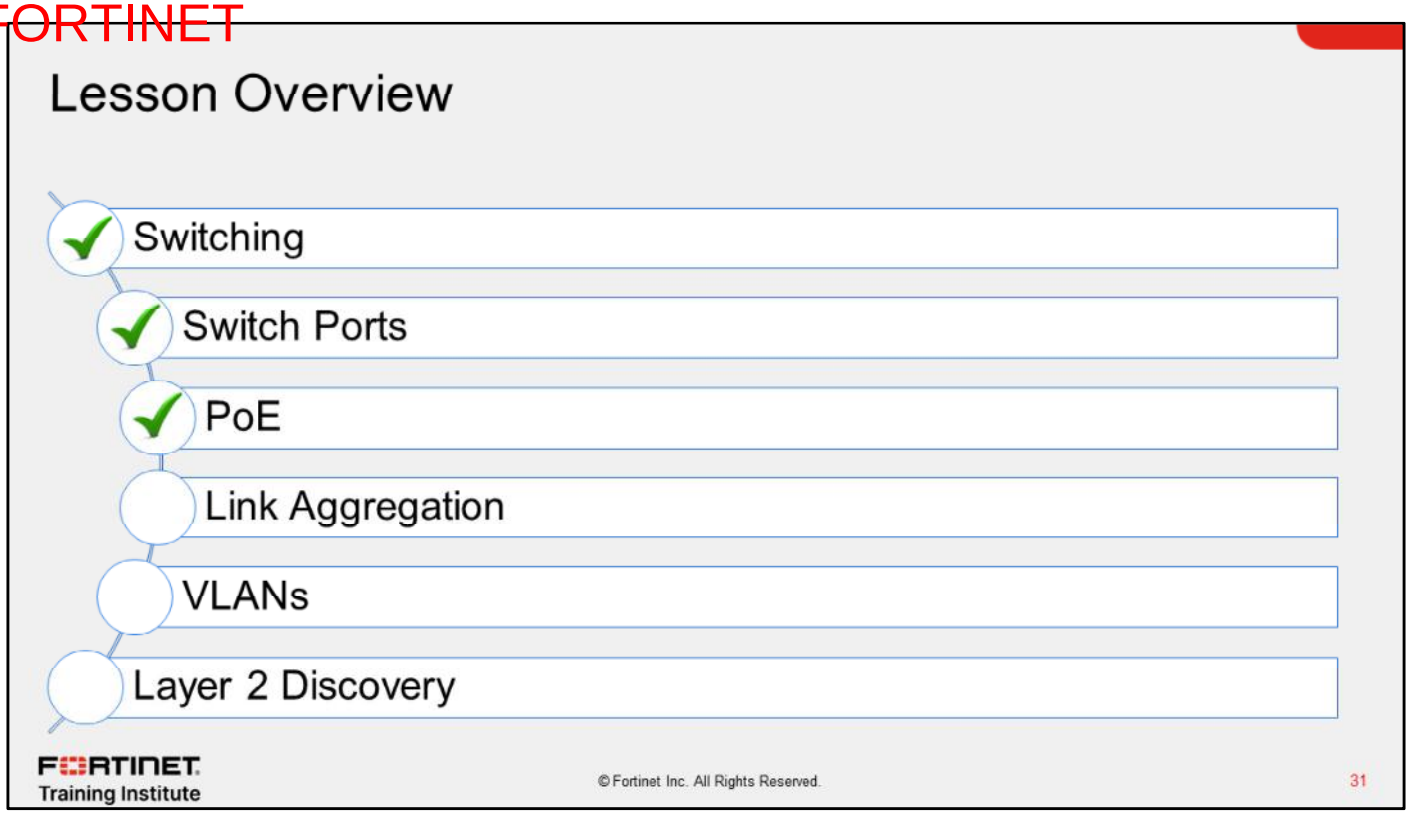
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

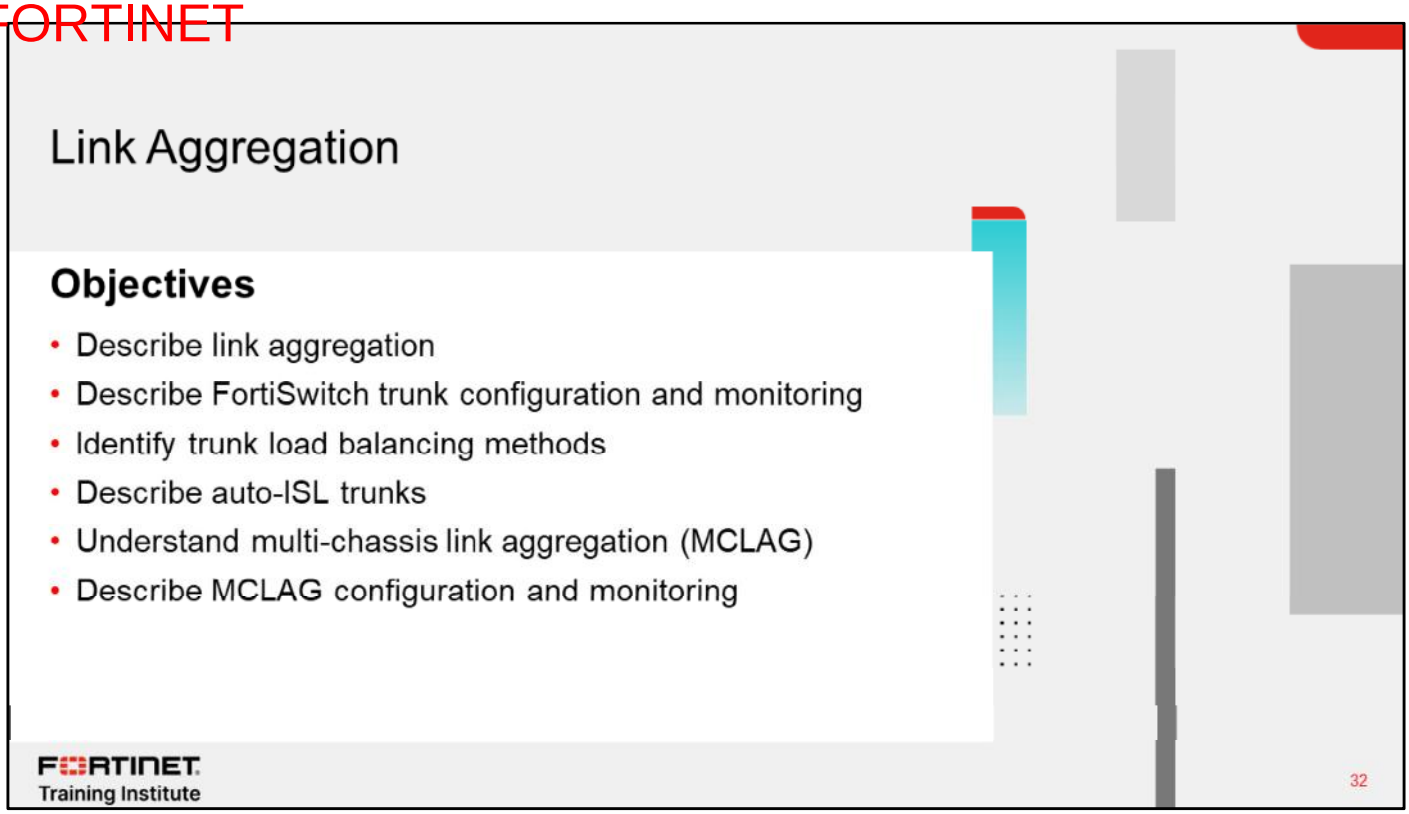


Good job! You now understand PoE.

Now, you will learn about link aggregation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

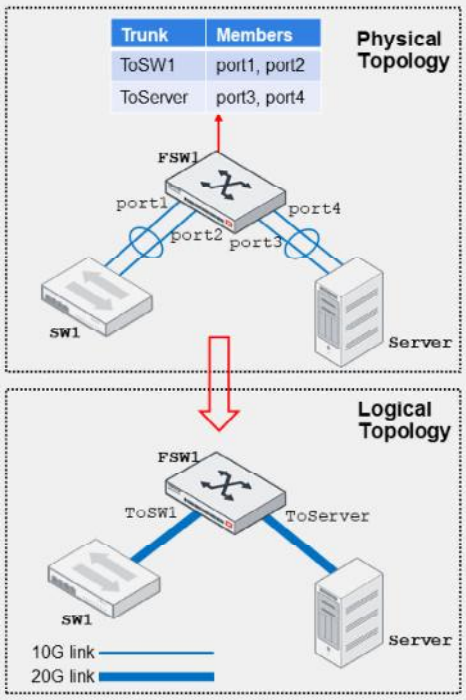
By demonstrating competence in link aggregation, you should be able to deploy FortiSwitch stacks that leverage the use of trunks to provide enhanced performance and redundancy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

What Is Link Aggregation?

- Combine multiple ports to create LAGs for:
  - Redundancy
    - Traffic fails over to another link on failure
  - Higher performance
    - Frames are load balanced across all members
- FortiSwitch refers to LAGs as trunks
- Two type of trunks:
  - Static
    - LAGs operate based on configuration
  - Dynamic
    - LACP negotiates members and detects failures
- Trunk creation
  - Automatic (auto-ISL)
    - FortiSwitch to FortiSwitch, or FortiSwitch to FortiGate
  - Manual
    - FortiSwitch to third-party devices
    - Maximum number of LAG members varies among models



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

Link aggregation combines multiple network connections to achieve redundancy and higher performance. A group of network connections that are bundled together is called a link aggregation group (LAG). A LAG operates as a single logical interface through which frames are load balanced among all LAG members based on the load balancing (or hashing) algorithm selected.

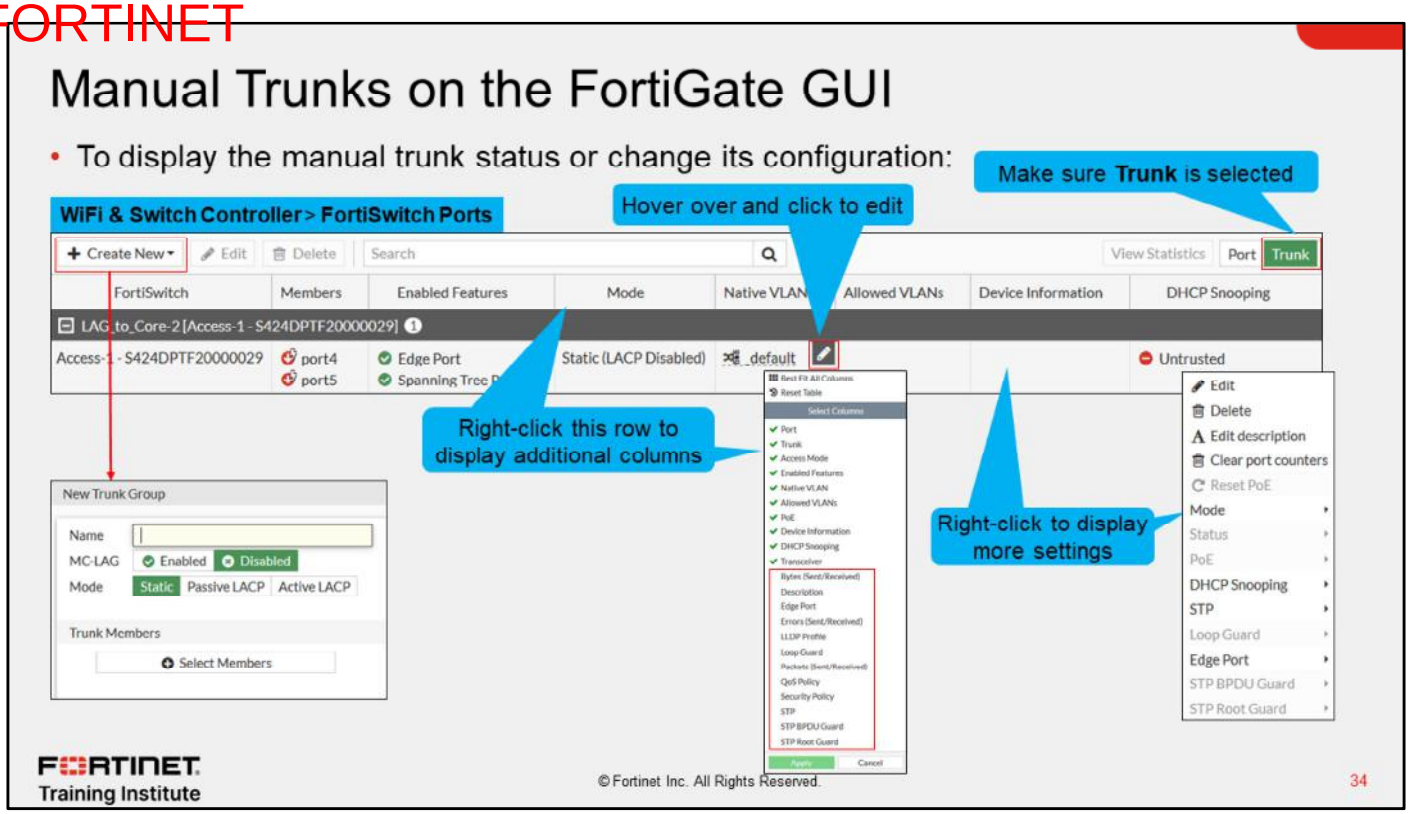
You can create static or dynamic LAGs. Static LAGs are formed based on the settings configured on each end. With dynamic LAGs, a control protocol, such as Link Aggregation Control Protocol (LACP), is used to automatically negotiate LAG members and perform failure detection. The result is that LAG members become active only after LACP determines that they are configured correctly and healthy. LACP is defined in IEEE 802.3ad and works by sending Link Aggregation Control Protocol Data Units (LACPDUs) on all LAG members. LACP supports two modes: active and passive. In active mode, LACP sends LACPDUs on all LAG members. In passive mode, a LAG member starts sending LACPDUs only after it receives LACPDUs from the adjacent port first.

In FortiSwitch, a LAG is referred to as a trunk. Although other vendors use the term trunk to refer to ports that accept tagged Ethernet frames, for FortiSwitch, a trunk is just a LAG. Trunks can be created automatically or manually. Automatic trunks are created on inter-switch links (ISLs) that connect FortiSwitch to another FortiSwitch, or FortiSwitch to FortiGate. You will learn more about auto-ISL in this lesson. Manual trunks are required for LAGs between FortiSwitch and third-party devices. Although trunks are often found in connections between network infrastructure devices, such as switches, firewalls, and routers, sometimes they are also used to connect servers and other endpoints that require enhanced redundancy and performance.

The example on this slide shows FortiSwitch (FSW1) with two LAGs: ToSW1 and ToServer. Each LAG has two 10G ports as members. From a logical point of view, the two LAGs work as two single interfaces, but with twice the bandwidth of their individual members.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On the FortiGate GUI, you can only configure manual trunks or edit existing ones. The configuration for auto-ISL trunks is displayed on the CLI only.

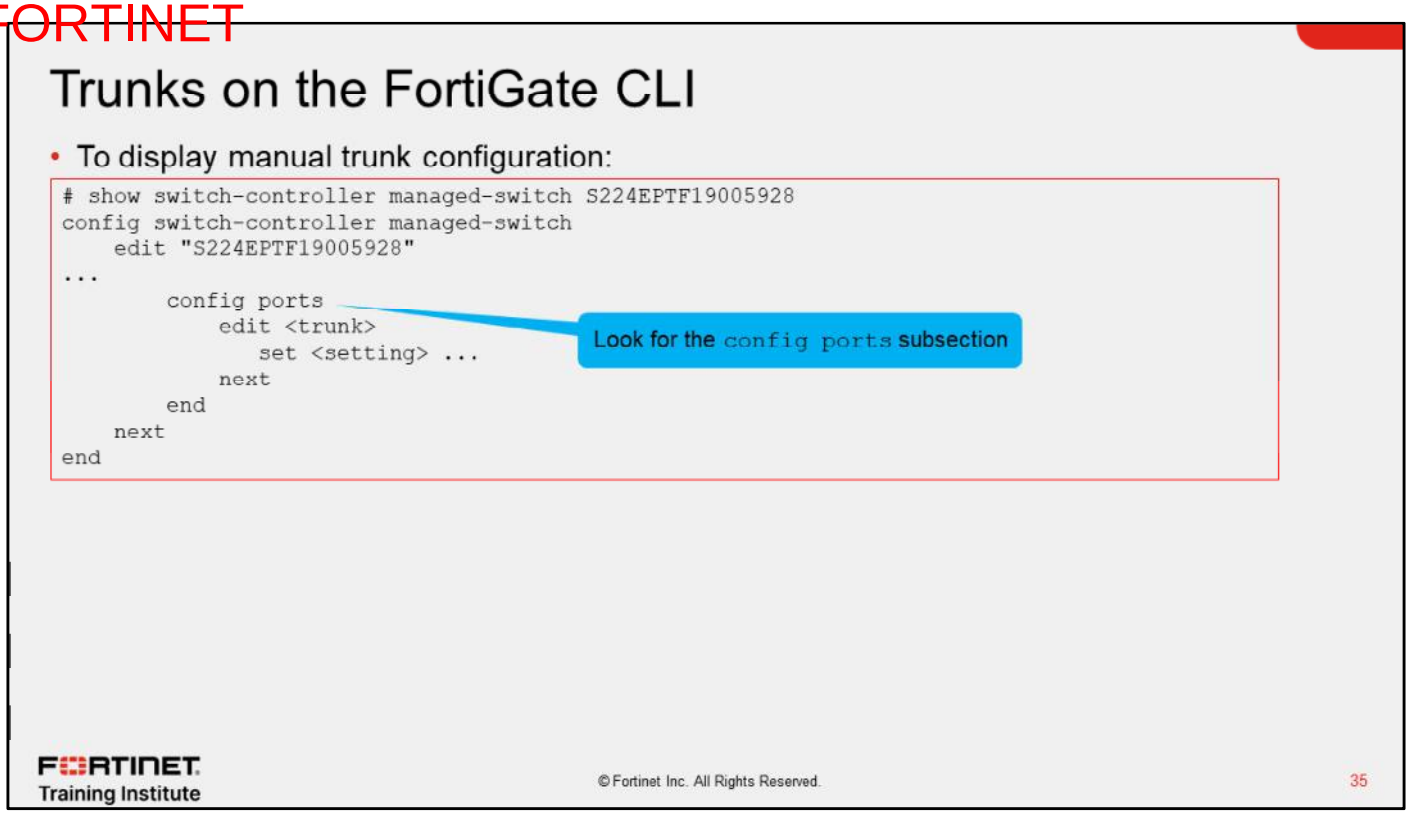
The **FortiSwitch Ports** page displays the configuration for manual trunks. Make sure the **Trunk** tab is selected. The information displayed on the page and the actions available are practically the same as in the **Port** tab. This is, you can edit the trunk configuration by hovering over the corresponding setting, right-clicking the top cell of any column to display a context menu with more available columns, or right-clicking a trunk row to display a context menu with some actions you can take.

To create a new trunk, click **Create New**. When you create a new trunk on the GUI, you must configure the following settings:

- **Name**: This is the LAG name.
- **MC-LAG**: MCLAG enables you to form a logical LAG with port members that connect to two different switches that are configured as MCLAG peers. You will learn more about MCLAG in this lesson.
- **Mode**: Select this if you want to create a static LAG, or a dynamic LAG using either passive or active LACP.
- **Trunk Members**: Select the ports that will be part of the LAG.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The manual trunk configuration of a managed switch can also be found in the `config ports` subsection under `config switch-controller managed-switch`. Use the `show` command to display the port configuration or navigate to the `config ports` subsection to edit one or more settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Trunks on the FortiGate CLI (Contd)

- To display the configuration for all trunks:

```
# diagnose switch-controller switch-info trunk config S224EPTF19005928
Vdom: root

S224EPTF19005928:
config switch trunk
    edit "GVM1V0000141680"
        set port-selection-criteria src-dst-ip
        set description ''
        set mode lacp-active
        set member-withdrawal-behavior block
        set bundle disable
        set auto-isl 1
        set fortilink 1
        set isl-fortilink 0
        set mclag disable
        set mclag-icl disable
            set members "port24"
        set lacp-speed slow
        set aggregator-mode bandwidth
    next
...
```

Load balancing method

LACP mode

1 = Auto-ISL trunk

1 = FortiLink trunk created using FortiLink protocol discovery

1 = FortiLink trunk created using LLDP protocol discovery

LAG members

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

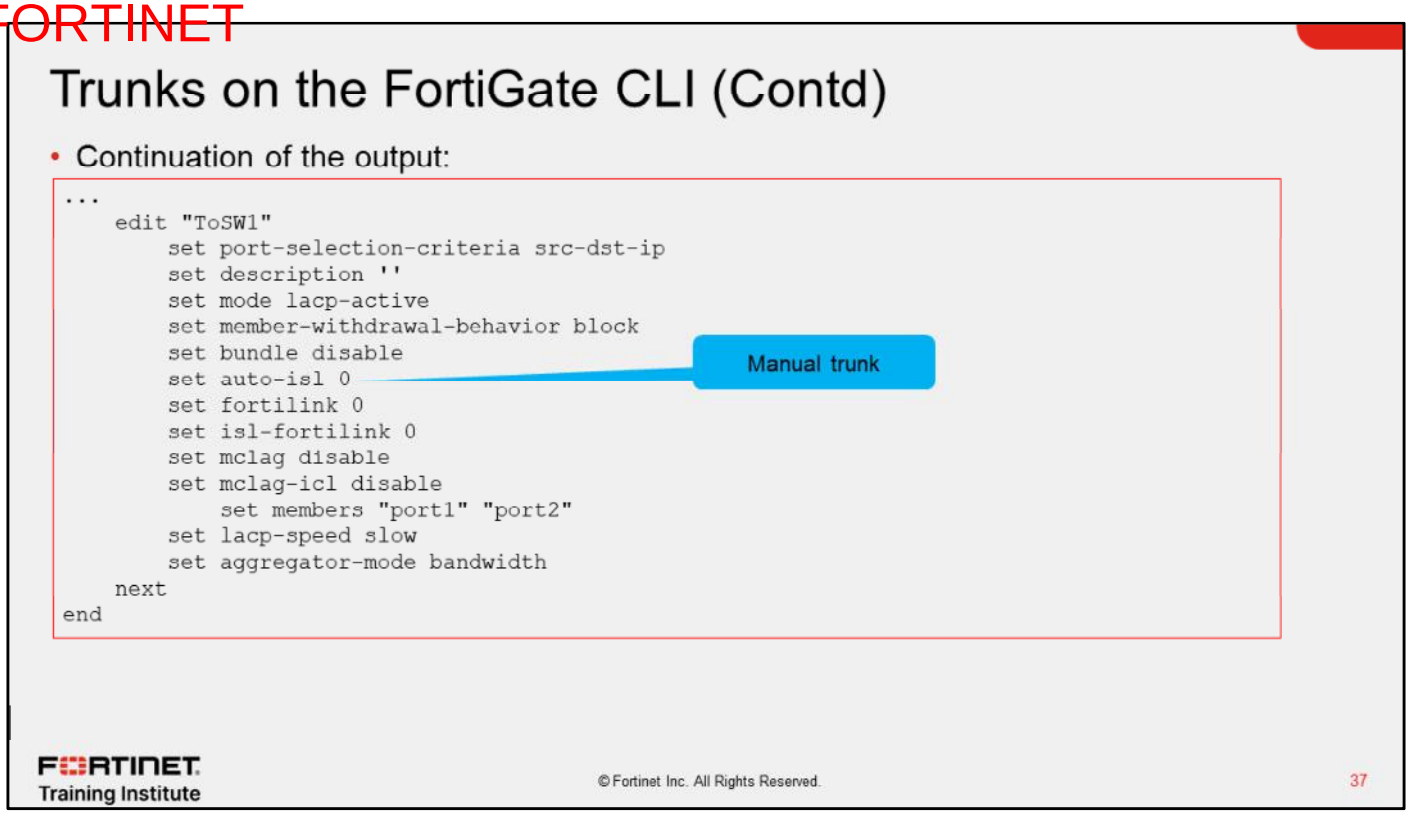
You can display the configuration for both manual and automatic trunks on the CLI by running the command shown on the slide. The output has been cut so it fits on the slide.

In the example output, `auto-isl` is set to `1`, which indicates that the trunk is an auto-ISL trunk. `fortilink` is set to `1`, which indicates that the trunk is a FortiLink trunk that was created on a switch that was discovered using the FortiLink protocol. By default, FortiGate discovers FortiSwitch devices using the FortiLink protocol, but you can also use LLDP as an alternative. When FortiSwitch is discovered using LLDP, `isl-fortilink` is set to `1` in the FortiLink trunk configuration.

Note that a FortiLink trunk shows a value of `1` for either the `fortilink` or the `isl-fortilink` setting, but *not* for both. FortiSwitch uses `auto-isl`, `fortilink`, and `isl-fortilink` settings for informational purposes only, and these settings are not meant to be changed by the administrator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a continuation of the output of the command on the previous slide. It shows the configuration for a manual trunk.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Trunks on the FortiGate CLI (Contd)

- Basic trunk status:

```
# execute switch-controller get-conn-status S224EPTF19005928
...
Aggregate Interfaces:

              Interface    Status    Duplex      Speed          Type
     4DPTF20000029-0(*)         up      full  1000Mbps           ISL
     4DPTF20000051-0(*)         up      full 10000Mbps           ISL
     GVM02TM21006376(*)         up      full  1000Mbps            FL
       _FlInK1_ICL0_(*)         up      full 10000Mbps           ICL

ISL: Inter-Switch-Link trunk.
FL: Fortilink Trunk connected to FGT.
(*): System auto generated trunk
```

- Detailed trunk status:

```
# diagnose switch-controller switch-info trunk status <switch-id> <trunk>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

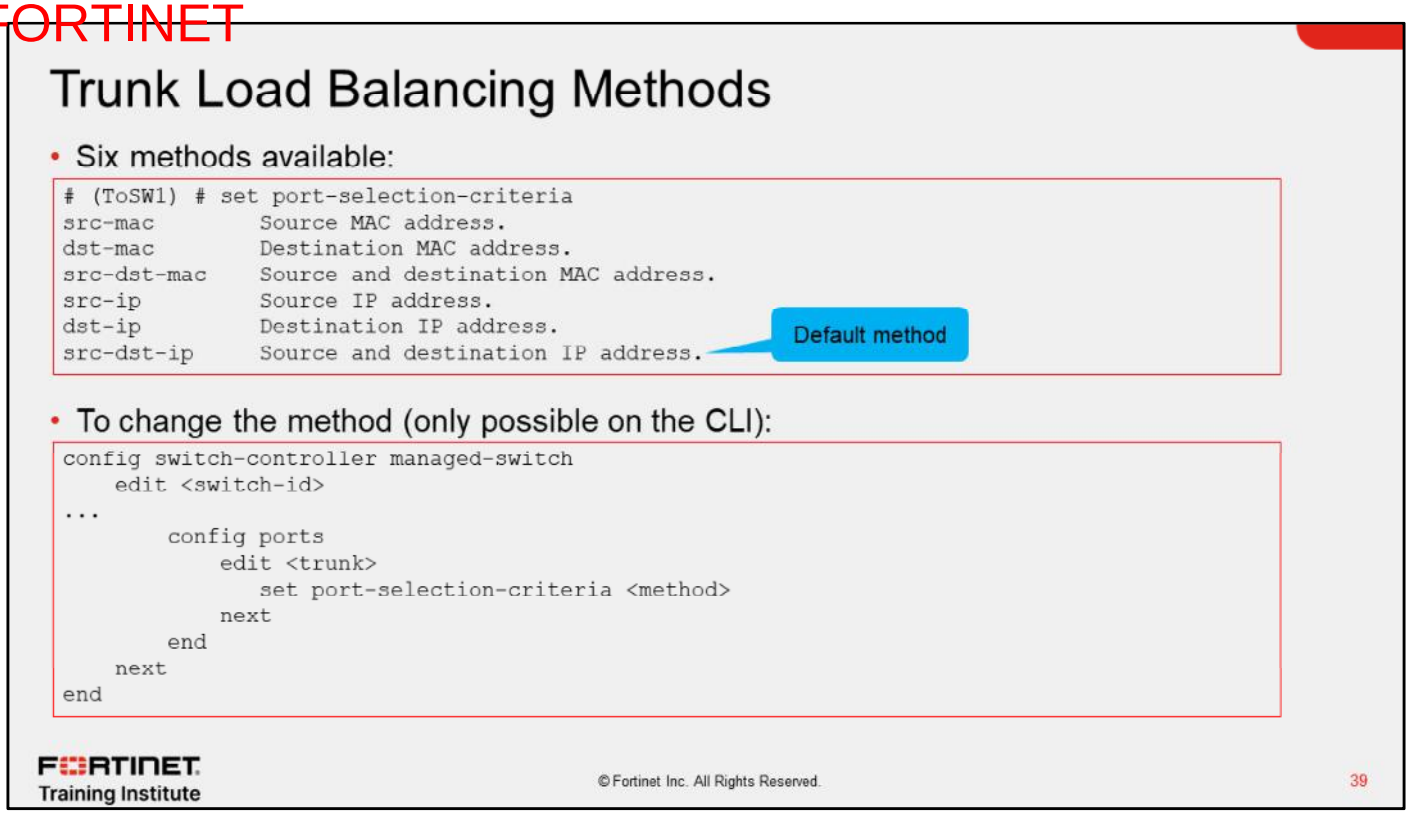
38

The FortiSwitch ports page on FortiGate shows basic status information about trunks. For this reason, the best way to get the status for trunks is to use the CLI. The output of the `execute switch-controller get-conn-status <switch-id>` command includes a section, at the end, with basic status information for both manual and auto-ISL trunks.

You can also see detailed status information about trunks by running the command shown on this slide. You will learn more about the output that this command generates in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



LAGs provide enhanced performance because they balance traffic across all members.

This slide shows the six load balancing methods available on a FortiSwitch trunk. The load balancing method, also known as the hashing algorithm or port selection criteria, determines the member to send a frame through, based on the MAC and IP addresses in the frame.

The default method is `src-dst-ip`, and it usually offers the best even distribution and works well for most environments. However, you can change the load balancing method on the FortiGate CLI by running the commands shown on this slide. For example, if your Ethernet traffic carries non-IP packets such as AppleTalk, Internetwork Packet Exchange (IPX), then it's better to use hashing algorithms that are MAC-based only. Another example is when Ethernet traffic uses QinQ tagging, in which case, it is also convenient to use a MAC-based load balancing method because FortiSwitch does not look at the inner Layer 3 protocol of a QinQ frame.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

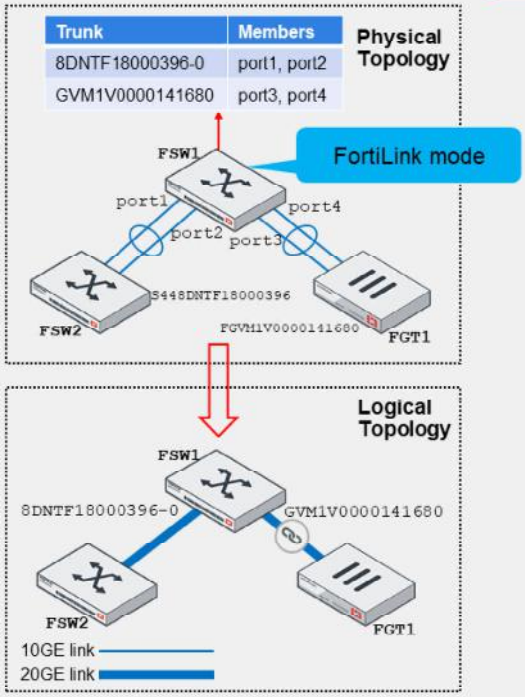
Auto-ISL

- A trunk is created automatically for ISLs and FortiLink trunks
  - At least one device must be a switch in FortiLink mode
  - Relies on LLDP for partner discovery and monitoring
  - FortiLink trunk's LACP mode matches FortiLink interface's
  - Trunk name contains the SN of the adjacent device
- To enable auto-ISL (enabled by default on all ports):

```
config switch-controller managed-switch
    edit <switch-id>
        config ports
            edit <port-id>
                set lldp-profile default-auto-isl
            next
    next
end
config switch-controller lldp-profile
    edit default-auto-isl
        set auto-isl enable
    next
end
```

Can't be disabled

- Auto-ISL trunks are deleted when they time out



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

Auto-ISL enables FortiSwitch to automatically create trunks on switch ports connecting to the FortiLink interface, and on switch ports used for ISLs. For auto-ISL to work, at least one end of the link must be connected to a FortiSwitch working in FortiLink mode. FortiSwitch detects the devices using Link Layer Discovery Protocol (LLDP). You will learn more about LLDP in this lesson.

When FortiSwitch connects to the FortiLink interface, it automatically creates the FortiLink trunk, which is technically also an auto-ISL trunk. The LACP mode on the FortiLink trunk automatically matches the LACP mode on the FortiLink interface, so there is no need for the administrator to manually indicate the LACP mode on the FortiLink trunk. If you connect two FortiSwitch devices, the LACP mode on both ends of the auto-ISL trunk is set to active mode by default, and therefore, no user intervention is required.

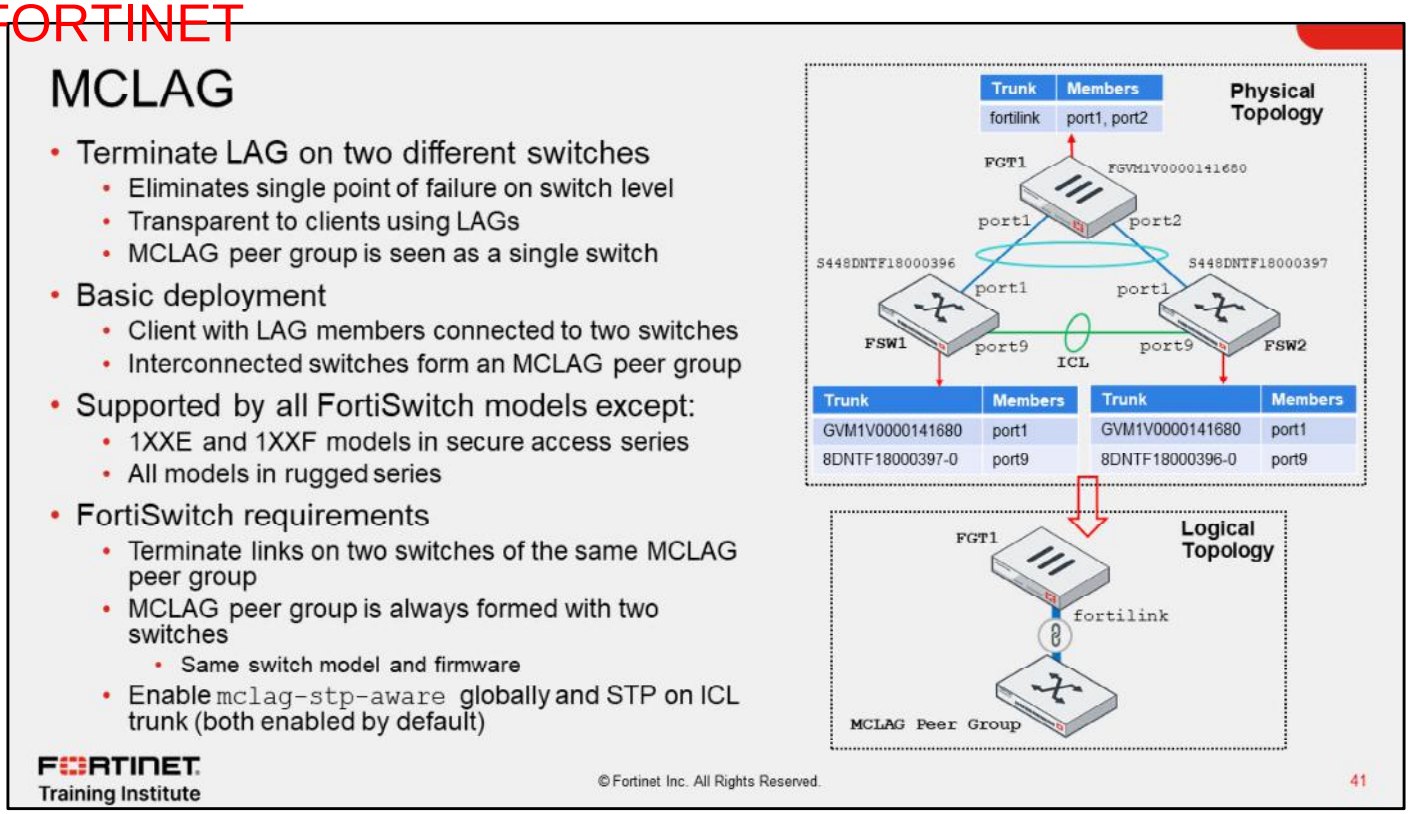
The members of an auto-ISL trunk are the ports that receive LLDP frames from the same adjacent device. In addition, FortiSwitch uses part of the adjacent device serial number to name the trunk. Auto-ISL works out of the box because all FortiSwitch ports are assigned with the `default-auto-isl` LLDP profile by default, which has the `auto-isl` option enabled by default.

After a trunk is formed automatically, the switch monitors the LLDP hello frames received from the adjacent device. If the adjacent device is a FortiSwitch in managed mode, the switch receives LLDP frames every three seconds by default. If the adjacent device is a FortiGate, the frames are received every 30 seconds. If FortiSwitch stops receiving LLDP frames for a certain period, it automatically removes the auto-ISL trunk from the configuration. The trunk deletion timeout is often 10 minutes or less and is set by FortiSwitch based on the configuration.

If you want to disable auto-ISL on a port, you must assign an LLDP profile to the port with the `auto-isl` setting disabled. Note that you cannot disable the `auto-isl` setting on the `default-auto-isl` profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A LAG combines multiple links that terminate on the same switch. Although LAGs provide higher bandwidth and redundancy, the fact that all links terminate on the same switch makes the LAG still susceptible to a single point of failure. This is, if you lose the switch, you also lose all your links. MCLAG overcomes this limitation by enabling you to form a LAG with links that terminate on *two different switches*. Adjacent network devices see the two switches as a single switch.

The most basic MCLAG deployment involves two switches and a client, such as FortiGate. The switches are connected through a LAG of one or more links to form an MCLAG peer group. The LAG that connects the switches is called the inter-chassis link (ICL), and is used to forward user traffic, as well as to exchange control information about the MCLAG. The client is configured with two links, each connected to a different switch. The switches work together so the LAG on the client operates like a regular LAG despite its links terminating on different switches. The result is that, if a link or a switch is lost, the switches coordinate with each other to ensure that the user traffic continues to be forwarded through the remaining active links.

All FortiSwitch models, except the ones indicated on this slide, support MCLAG. MCLAG is a vendor-specific implementation, and in the case of FortiSwitch, has the following requirements:

- The switches where the links terminate must be configured as MCLAG peers.
- An MCLAG peer group is formed with two switches. The switches in the MCLAG peer group must be of the same hardware model and same software version.
- `mclag-stp-aware` must be enabled globally on FortiSwitch, and STP must be enabled on the ICL trunk. Both settings are enabled by default.

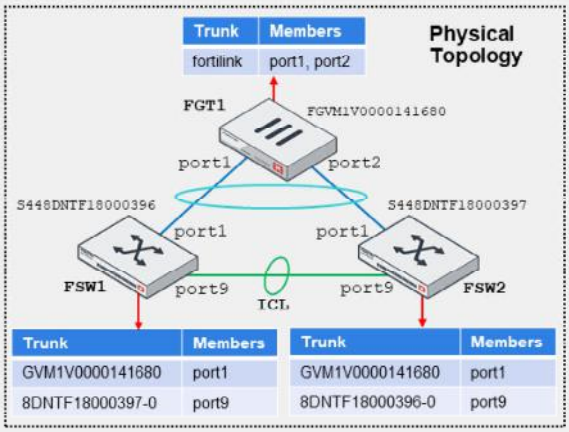
The example on this slide shows a basic MCLAG setup. The fact that the FortiLink interface is connected to two switches is transparent to FortiGate. As a result, FortiGate sees the LAG as a regular LAG.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Basic FortiLink MCLAG Configuration

1. Enable FortiLink split interface (optional)
   - Prevents service disruption
   - Omit if:
     - Using console to access switches and
     - Service disruption is acceptable
2. Enable `mclag-icl` on the ICL trunk
   - Requires access to switch CLI
   - Start with FSW2 (switch terminating second link)
3. Disable FortiLink split interface
   - Required for MCLAG negotiation to complete



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

The basic FortiLink MCLAG deployment shown on this slide is one of the multiple MCLAG topologies FortiSwitch supports. FortiGate, acting as the client, terminates its FortiLink interface in two switches that are configured as MCLAG peers. After you make the physical connections shown on this slide, and assuming switches are authorized and online, you can configure the MCLAG as follows:

1. Enable FortiLink split interface on the FortiLink interface.
This setting is enabled by default and instructs FortiGate to keep only the first FortiLink member active, while keeping the second inactive. Based on the example topology, port1 and port2 are considered the first and second FortiLink members, respectively. By keeping only one link active, you ensure that you can connect to both switches over SSH from FortiGate to configure MCLAG, and that user traffic is not impacted. Otherwise, you lose the management connection to one of the switches, and cause a service disruption in the network. If you have console access to the switches and don't care about network disruption, you can omit this step.

2. Enable `mclag-icl` on the ICL trunk.
You must configure this setting on the switch CLIs. If you access them from FortiGate, enable the setting first on the ICL trunk of the switch that terminates the second FortiLink interface link (FSW2 in the example), and then enable it on the ICL trunk of the other switch (FSW1). This order of execution avoids losing network access to the switches. If you connect to the switch CLIs over the console, the order does not matter. The ICL trunk should be formed on each switch automatically because of auto-ISL. If there are multiple trunks, identify the ICL trunk by its name, which should match the serial number of the adjacent switch, or by looking at its port member (port9 in the example).

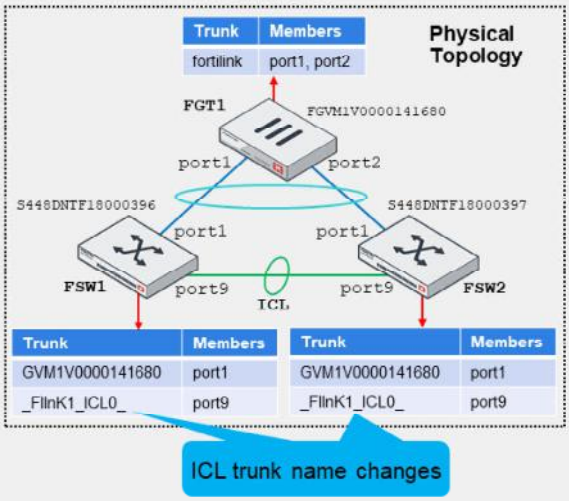
3. Disable FortiLink split interface on the FortiLink interface.
Both FortiLink members must be active for MCLAG negotiation to complete.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MCLAG ICL Configuration Using LLDP Profiles

1. Enable FortiLink split interface (optional)
   - Prevents service disruption
2. Set `default-auto-mclag-icl` LLDP profile on ICL members
   - Available on the FortiGate CLI
3. Disable FortiLink split interface
   - Required for MCLAG negotiation to complete



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

43

In the previous procedure, you had to connect to the FortiSwitch CLI to manually enable `mclag-icl` on the ICL ports. An alternative is to use the FortiGate CLI to set the `default-auto-mclag-icl` LLDP profile on the ICL ports. This LLDP profile is one of the default LLDP profiles that are created on the FortiGate on FortiSwitch discovery. It instructs FortiSwitch to automatically enable `mclag-icl` on the auto-ISL trunk that contains the port that has the LLDP profile set. As a result, FortiSwitch creates the auto-ISL trunk with `mclag-icl` enabled, and assigns it the name shown on the slide. You will learn more about LLDP and the default LLDP profiles in this lesson.

The other steps in the procedure are the same as in the previous slide. This is, enable FortiLink split interface at the beginning, and then disable it at the end for MCLAG negotiation to complete.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about FortiSwitch trunks is true?
   - A. A trunk is a port that can send and receive tagged frames.
   - ✓ B. A trunk is a LAG.

2. Which protocol does auto-ISL use to identify adjacent FortiSwitch and FortiGate devices?
   - ✓ A. LLDP
   - B. LACP

3. Which setting must be enabled on ICL trunks to configure MCLAG?
   - ✓ A. `mclag-icl`
   - B. `mclag-stp-aware`

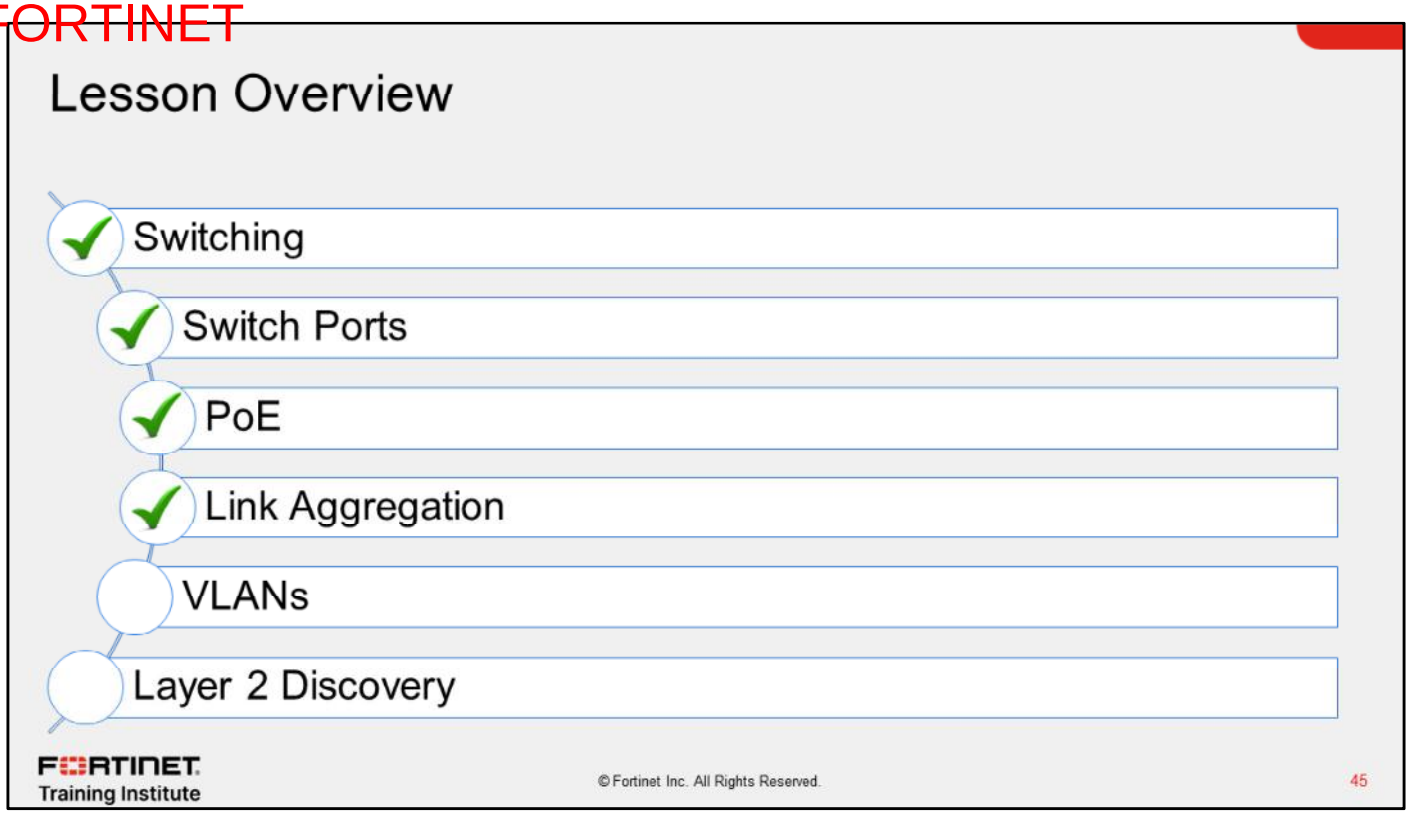
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

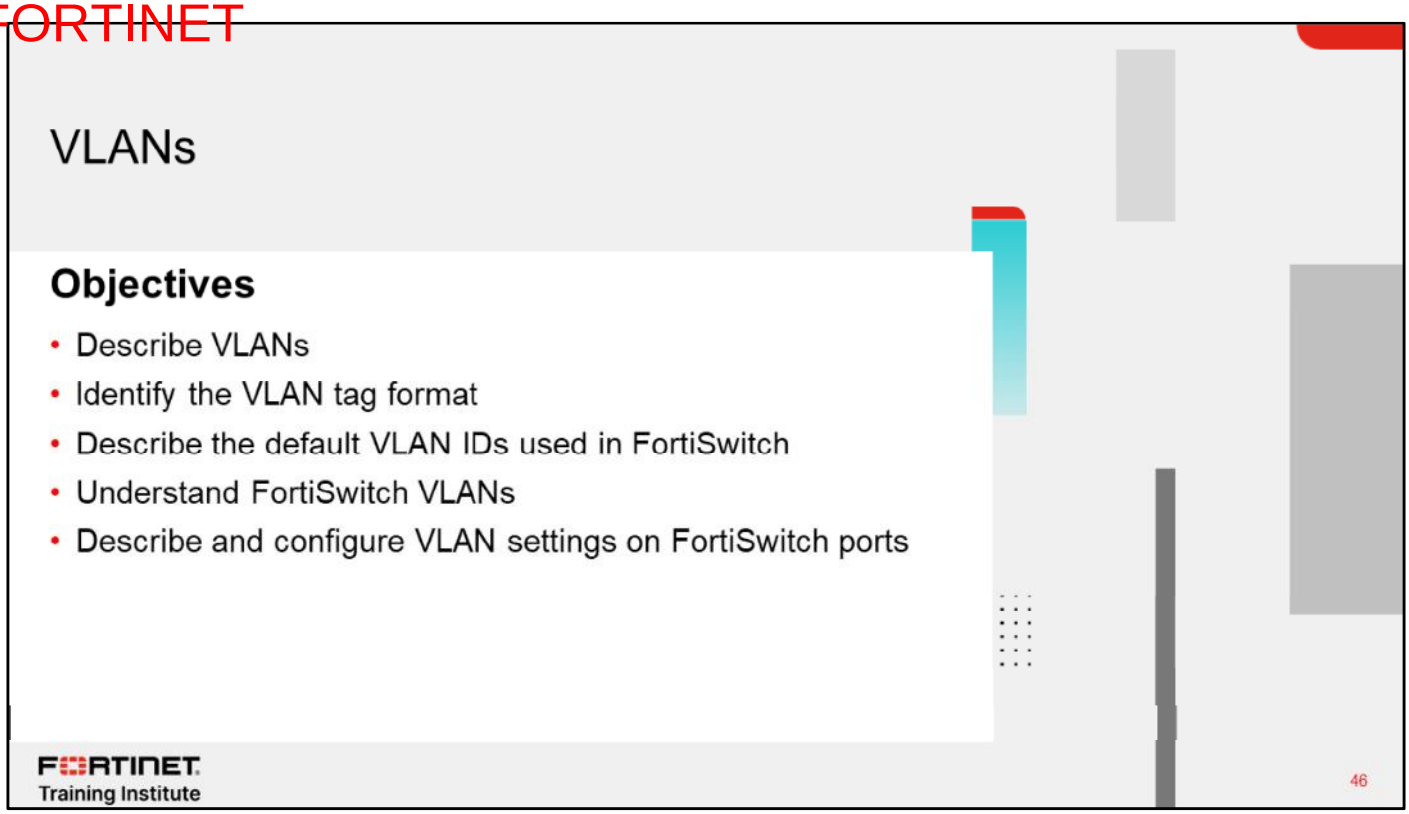


Good job! You now understand link aggregation.

Now, you will learn about virtual LANs (VLANs).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

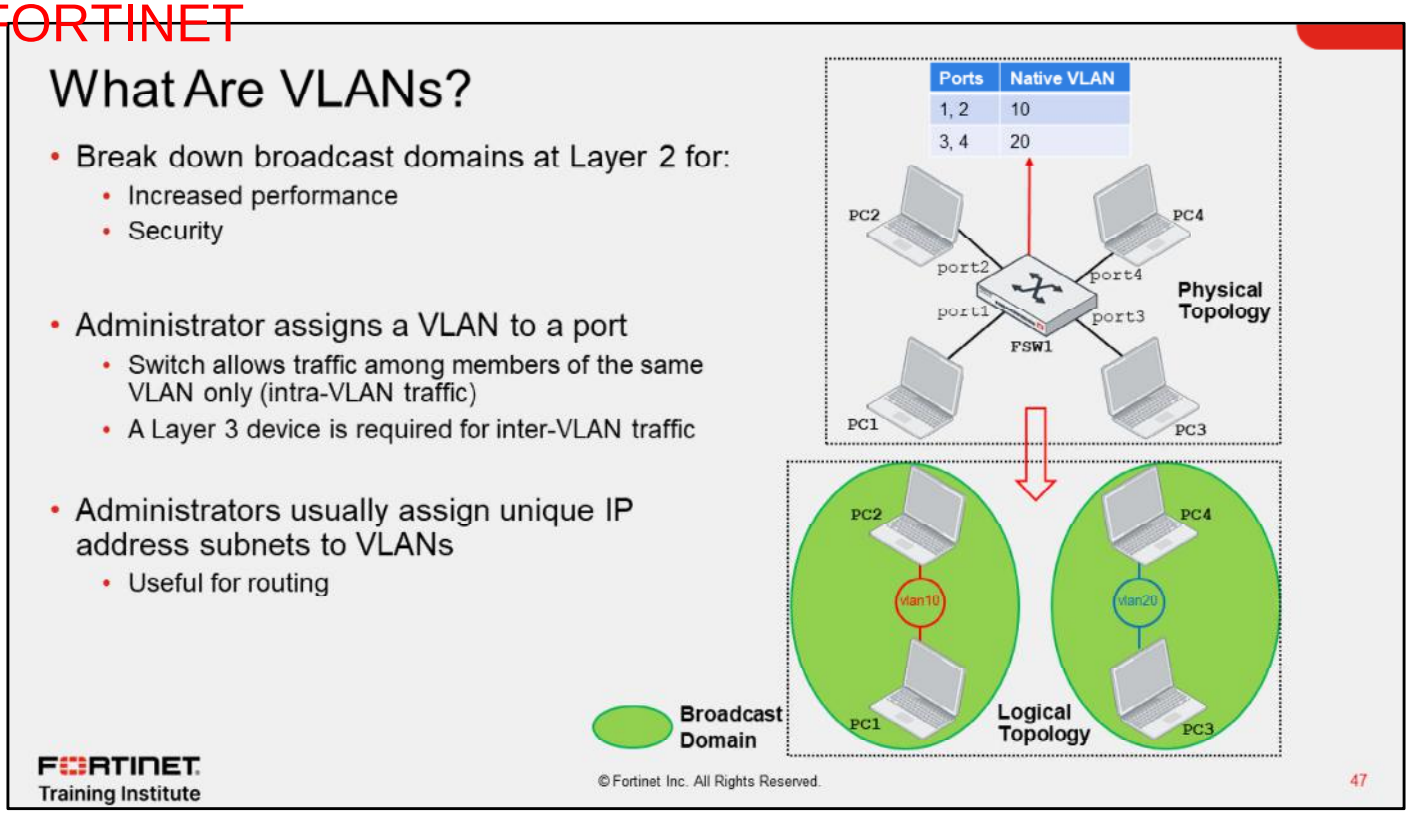


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in VLANs, you should be able to deploy VLANs in your switch stack for enhanced security and performance purposes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you connect devices to a switch, you break collision domains into smaller collision domains. However, all devices still belong to the same broadcast domain, which means that all devices can be reached. This means that not only will devices have to use valuable bandwidth and system resources to process some traffic that they may not really need to process, but there is also nothing stopping a device from reaching others in the broadcast domain. Using VLANs, administrators can logically group devices and isolate them for increased performance and security purposes.

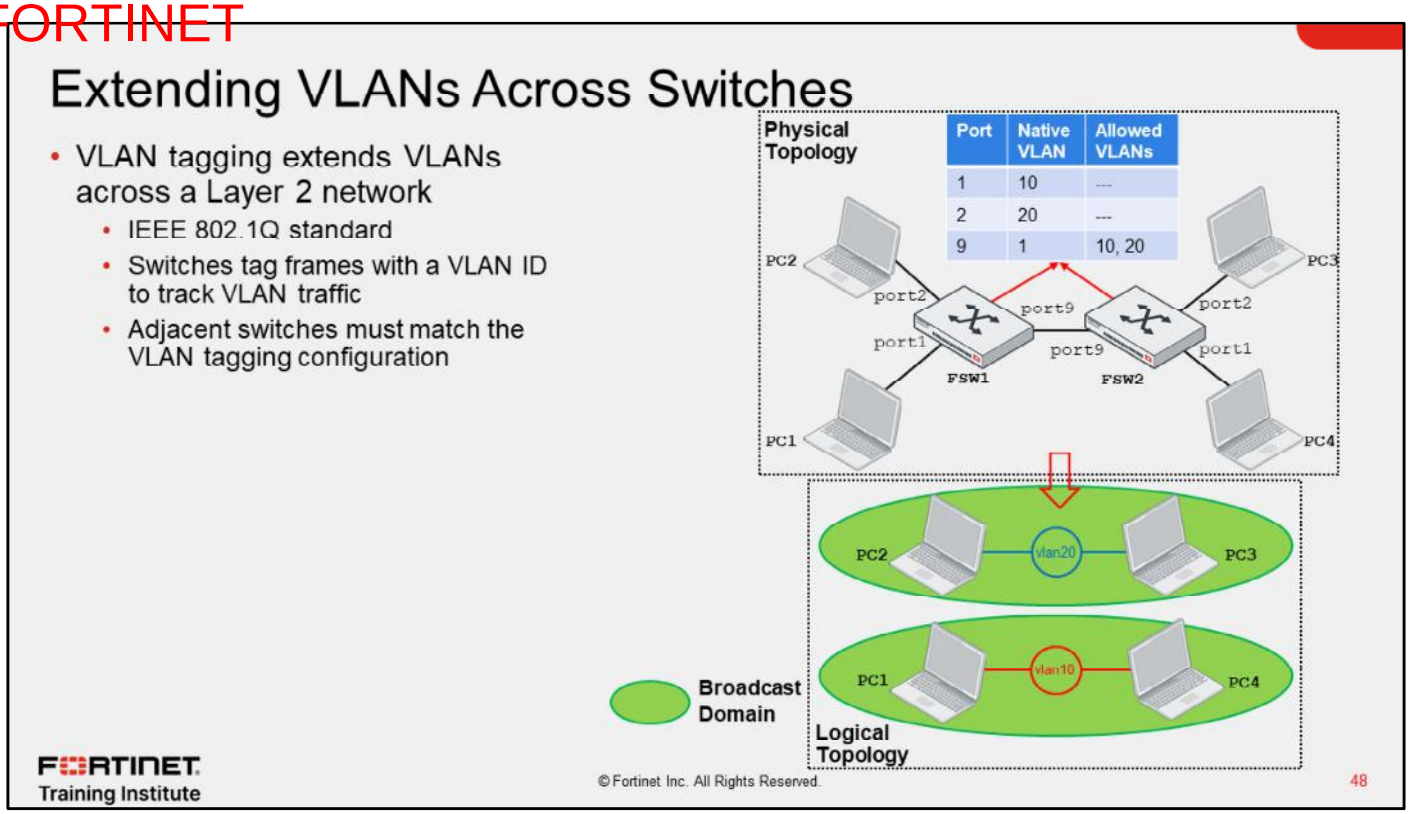
When you use VLANs, you are essentially instructing the switch to create additional broadcast domains at the Layer 2 network, and forward traffic between devices connected to switch ports belonging to the same VLAN only. This is called intra-VLAN traffic.

If devices assigned to different VLANs need to communicate—this is called inter-VLAN traffic—you require a Layer 3 device, such as a FortiGate or a router, to enable communication between the VLANs. As a best practice, you should assign unique IP address subnets to each VLAN. This avoids having to use NAT to route traffic between VLANs, which simplifies deployment and troubleshooting.

In the example shown on this slide, there are two topology views: physical and logical. The physical topology view shows how devices are physically connected to the switch, as well as the native VLAN configuration for the switch ports. You will learn more about native VLAN in this lesson, but for now, just think of it as the VLAN a device belongs to. According to the port configuration, port1 and port2 are assigned to VLAN 10, and port3 and port4 to VLAN 20. Therefore, a logical view of the topology would show that PC1 and PC2 can communicate with each other because they both belong to the same VLAN (VLAN 10). Similarly, both PC3 and PC4 belong to VLAN20 and therefore, can talk to each other. In addition, PCs that belong to different VLANs cannot talk to each other because they are isolated, by the switch, in separate broadcast domains.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



VLANs can also span multiple switches in a Layer 2 network. For this to work, switches add a tag to frames when they forward them to adjacent switches. The tag indicates the ID of the VLAN that the frames belong to. IEEE 802.1Q, often referred to as dot1q, is the networking standard that defines VLAN tagging for Ethernet frames and the way switches and other dot1q-compatible devices must handle these frames.

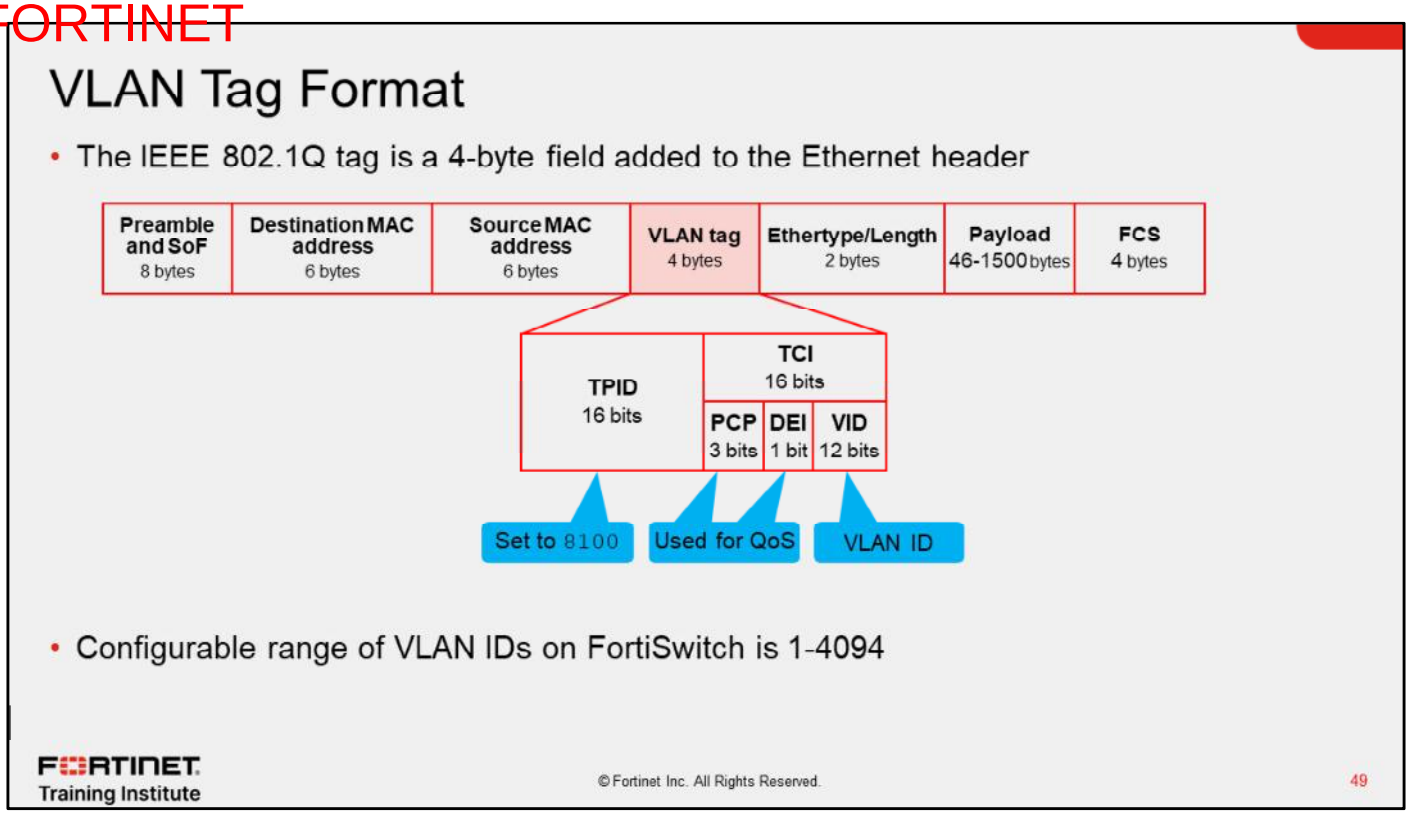
When an adjacent switch receives a tagged frame, it looks at the VLAN ID in the tag, and then forwards the frame to a port that is part of the same VLAN, and where the destination MAC address was recorded.

To make sure adjacent switches can process tagged traffic accordingly, you must ensure the ports connecting the inter-switch links (ISLs) have matching VLAN tagging settings. In FortiSwitch, the setting that controls the VLAN IDs accepted on a port is the **Allowed VLANs** setting. You will learn more about this setting in this lesson.

In the example shown on this slide, the two switches have the same port settings. port9 on each switch is used for the ISL. port9 settings allow traffic tagged with VLAN IDs 10 and 20 across the ISL. In addition, PC1 and PC4 are in VLAN 10, while PC2 and PC3 in VLAN 20. The resulting logical topology shows that PCs placed in the same VLAN can communicate with each other even though they are connected to different switches.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



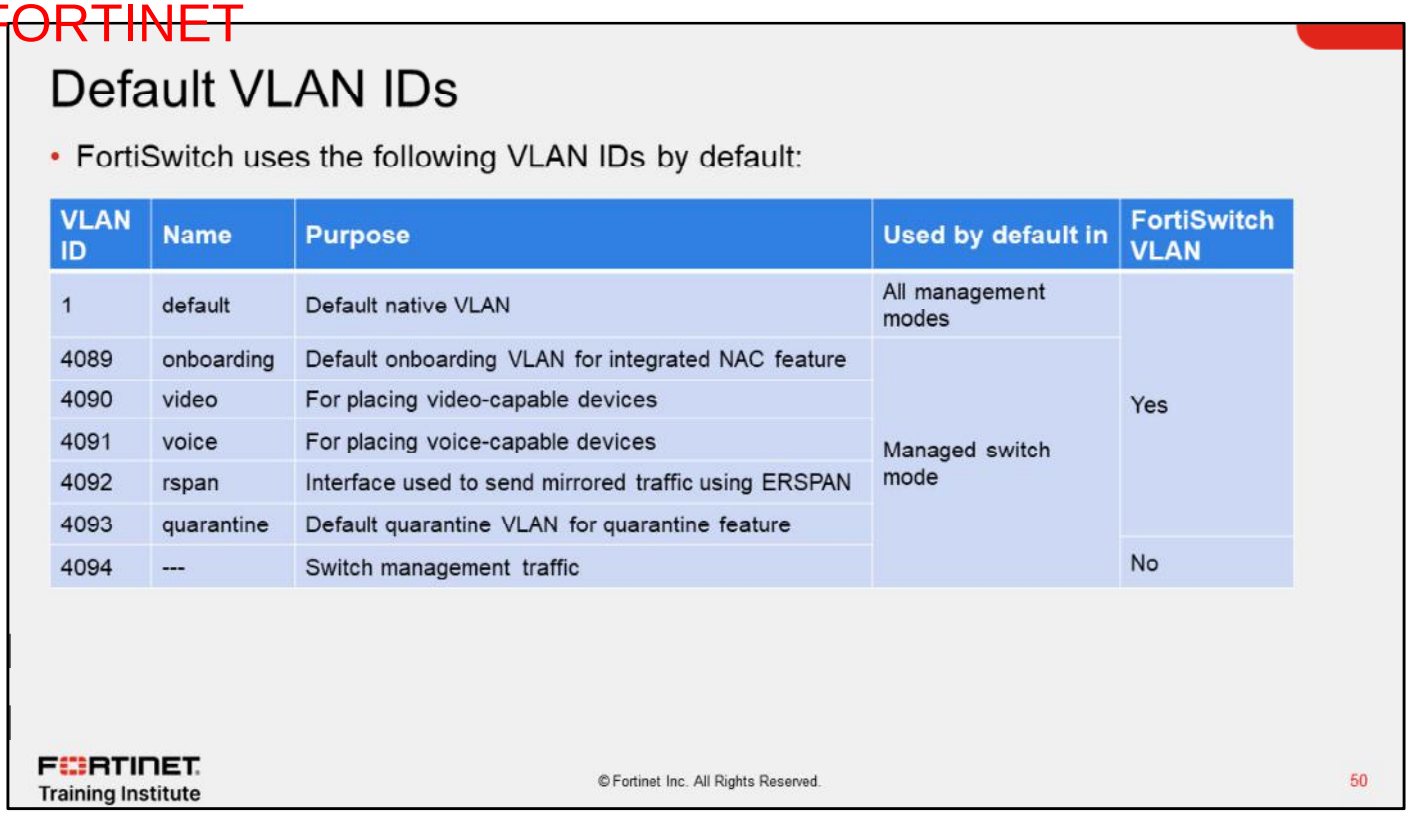
IEEE 802.1Q inserts a 4-byte field into the Ethernet header that contains the VLAN ID information, as well as other information that can be used for traffic marking and prioritization purposes when quality of service (QoS) is required.

The field is divided into two 16-bit halves: tag protocol identifier (TPID) and tag control information (TCI). The TPID is always `8100`, which indicates the type of the VLAN tag is 802.1Q. The TCI contains the following sub-fields:

- Priority code point (PCP): Refers to the IEEE 802.1p class of service, and is used to set a priority on frames. Switches configured with QoS policies look at this value to determine whether the frame should be expedited.
- Drop eligible indicator (DEI): Indicates whether the frame can be dropped during congestion.
- VLAN ID (VID): The ID of the VLAN the frame belongs to. A VLAN ID is a number in the 0–4095 range. FortiSwitch reserves the use of VLAN IDs 0 and 4095, so the actual configurable range on FortiSwitch is 1–4094.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



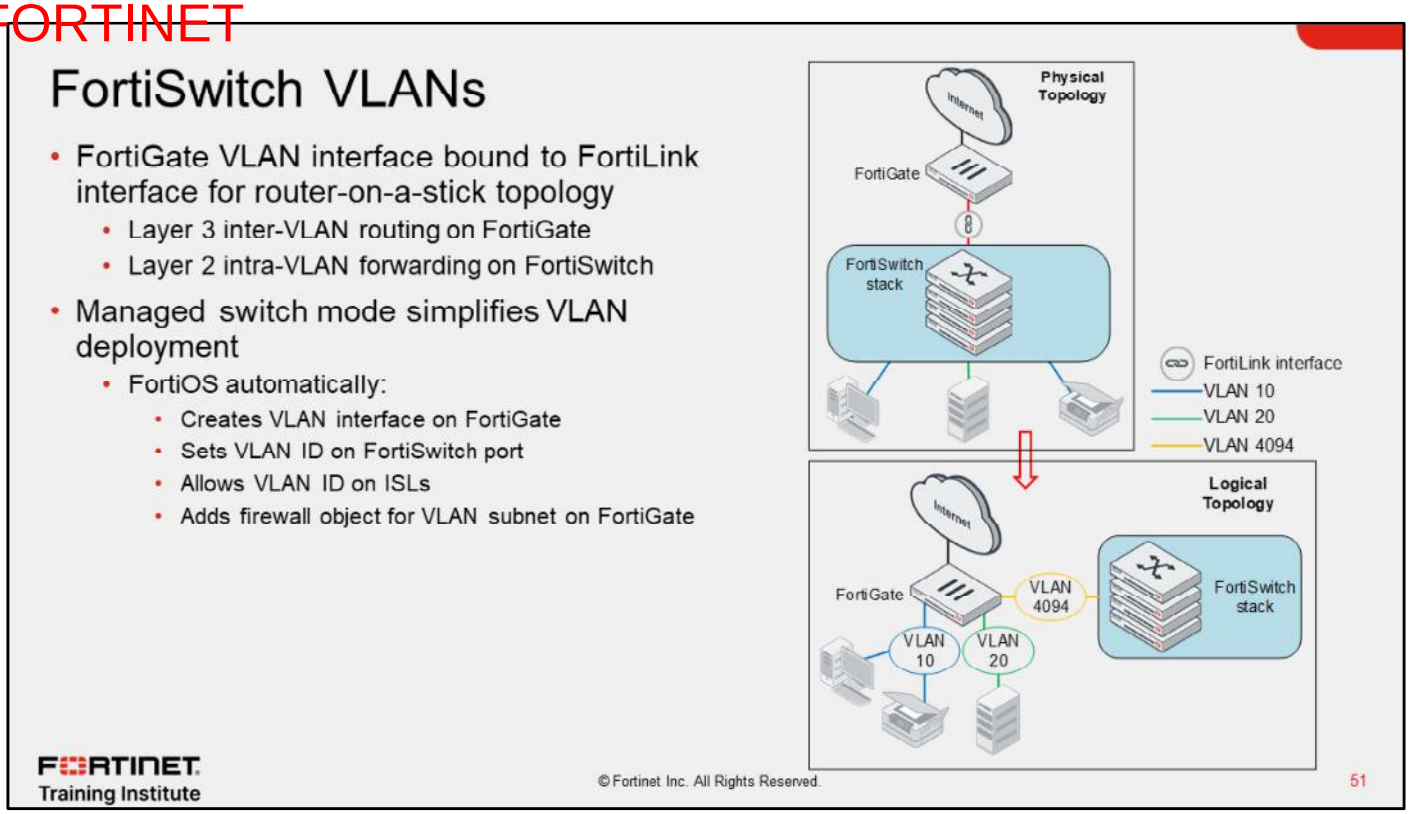
FortiSwitch uses some VLAN IDs are used by FortiSwitch by default. The table on this slide shows these VLAN IDs, and the management mode in which they are used.

All VLAN IDs are meant to be used for user traffic, except VLAN ID 4094, which is intended to be used for switch management traffic only. For this reason, FortiGate does not create a FortiSwitch VLAN using VLAN ID 4094.

Note that you can change the default VLAN IDs and their names to prevent a conflict with an existing configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A FortiSwitch VLAN is essentially a FortiGate VLAN interface that is bound to a FortiLink interface. The VLAN is then used for Layer 3 routing on FortiGate and for Layer 2 VLAN segmentation on FortiSwitch. The goal is to deploy a router-on-a-stick topology in which FortiGate handles inter-VLAN routing and FortiSwitch handles intra-VLAN forwarding.

When you manage FortiSwitch on FortiGate, you configure FortiSwitch VLANs, and assign them to switch ports. Although you can deploy a router-on-a-stick topology using FortiGate and third-party switches, when you use a FortiSwitch stack in managed switch mode, VLAN deployment is simplified considerably because FortiOS automatically takes care of the following:

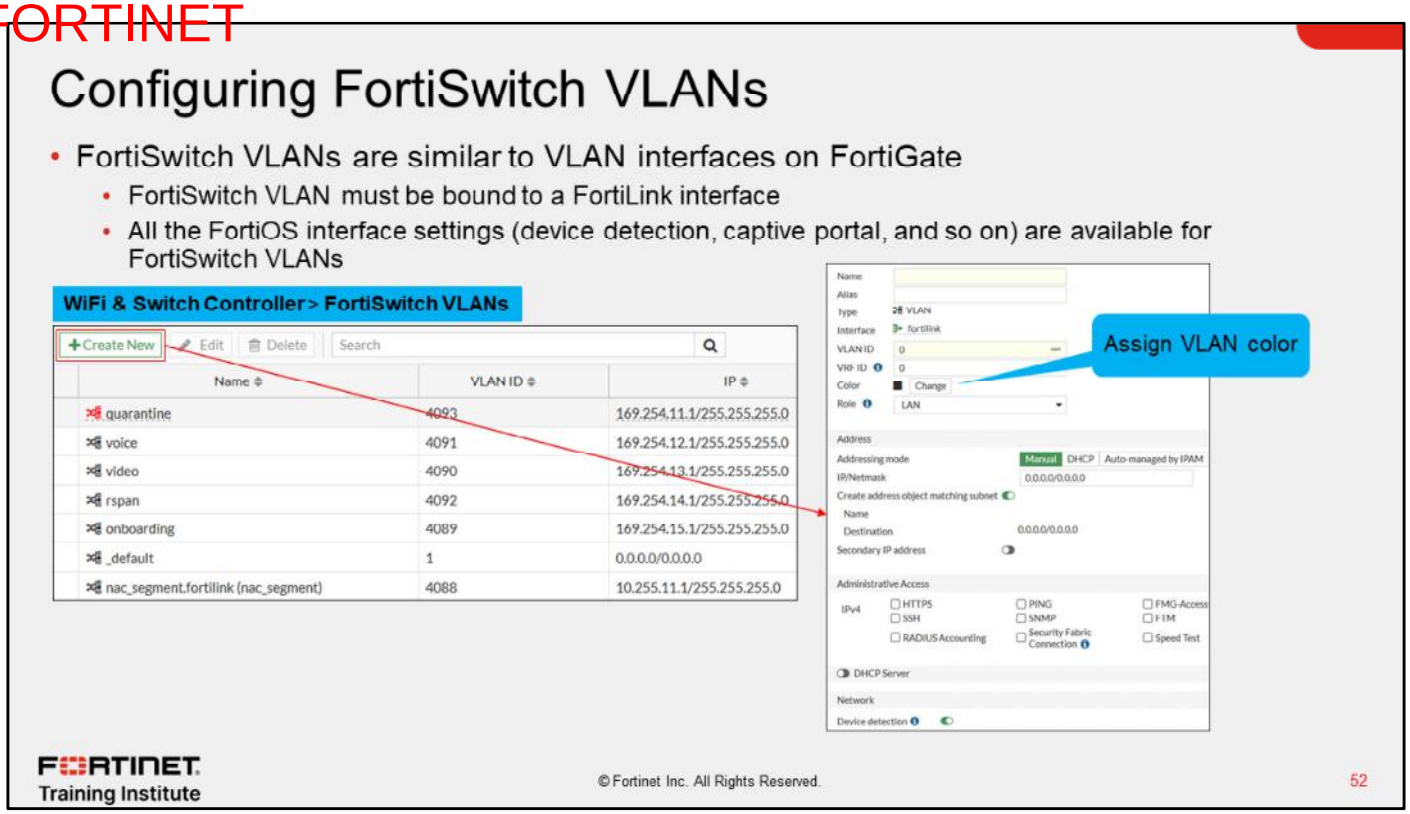
- Creating the VLAN interface on FortiGate
- Assigning the corresponding VLAN ID to the switch ports that belong to the VLAN
- Ensuring that the VLAN ID is allowed on the ISLs that connect adjacent switches, so traffic from multiple VLANs can span across the FortiSwitch stack
- Adding a firewall object for the IP subnet used for the FortiSwitch VLAN, so it can be referenced in firewall policies for controlling inter-VLAN traffic

If you were using third-party switches, you would have to do all of this configuration manually, which could result in a VLAN configuration mismatch and possible service impact.

The example on this slide shows the physical and logical topology views when using VLANs. Note that VLAN 4094 is the default switch management VLAN, and it's not available as a FortiSwitch VLAN on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



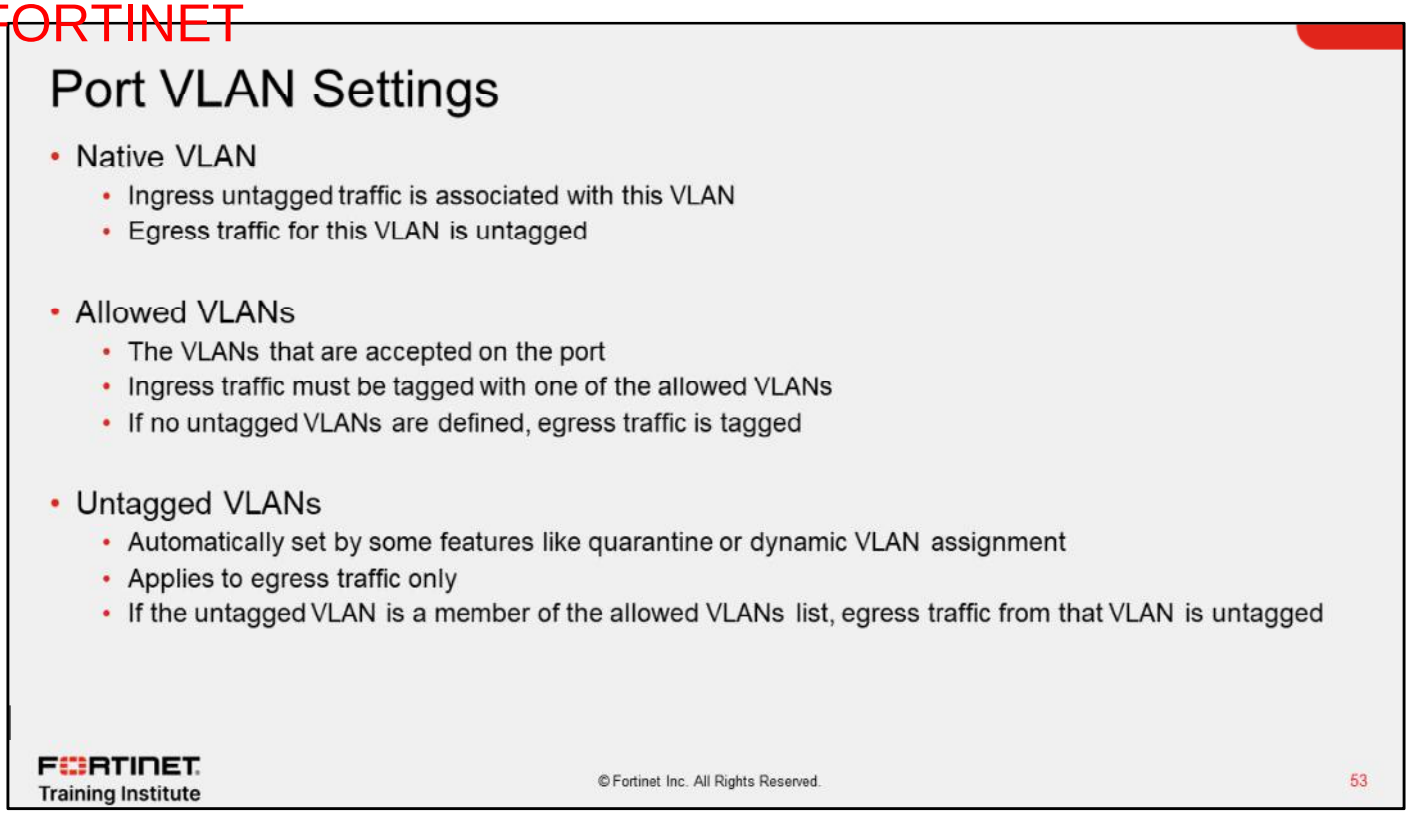
When you manage a switch stack on FortiGate, the switches become an extension of FortiGate. You configure and use FortiSwitch VLANs in the same way as FortiGate VLANs. Keep in mind that a FortiSwitch VLAN *must be* bound to a FortiLink interface. Otherwise, you won't be able to select the VLAN when you configure the VLAN settings on a switch port.

In addition, all interface settings usually available on FortiGate VLANs, are also available on FortiSwitch VLANs, such as device detection, captive portal, DHCP server, and so on.

One specific setting that is available for FortiSwitch VLANs only is **Color**. This setting enables you to assign a color to a VLAN, so when you review the switch port configuration on the GUI, you can quickly identify the VLANs assigned to the ports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiSwitch can process tagged and untagged Ethernet frames. When you configure a port, you must ensure that the port VLAN settings match the VLAN tagging required by the connected device for ingress and egress traffic. The following list describes the VLAN settings that define how the port handles tagged and untagged traffic. Note that ingress and egress traffic refer to the traffic entering and leaving the switch port, respectively.

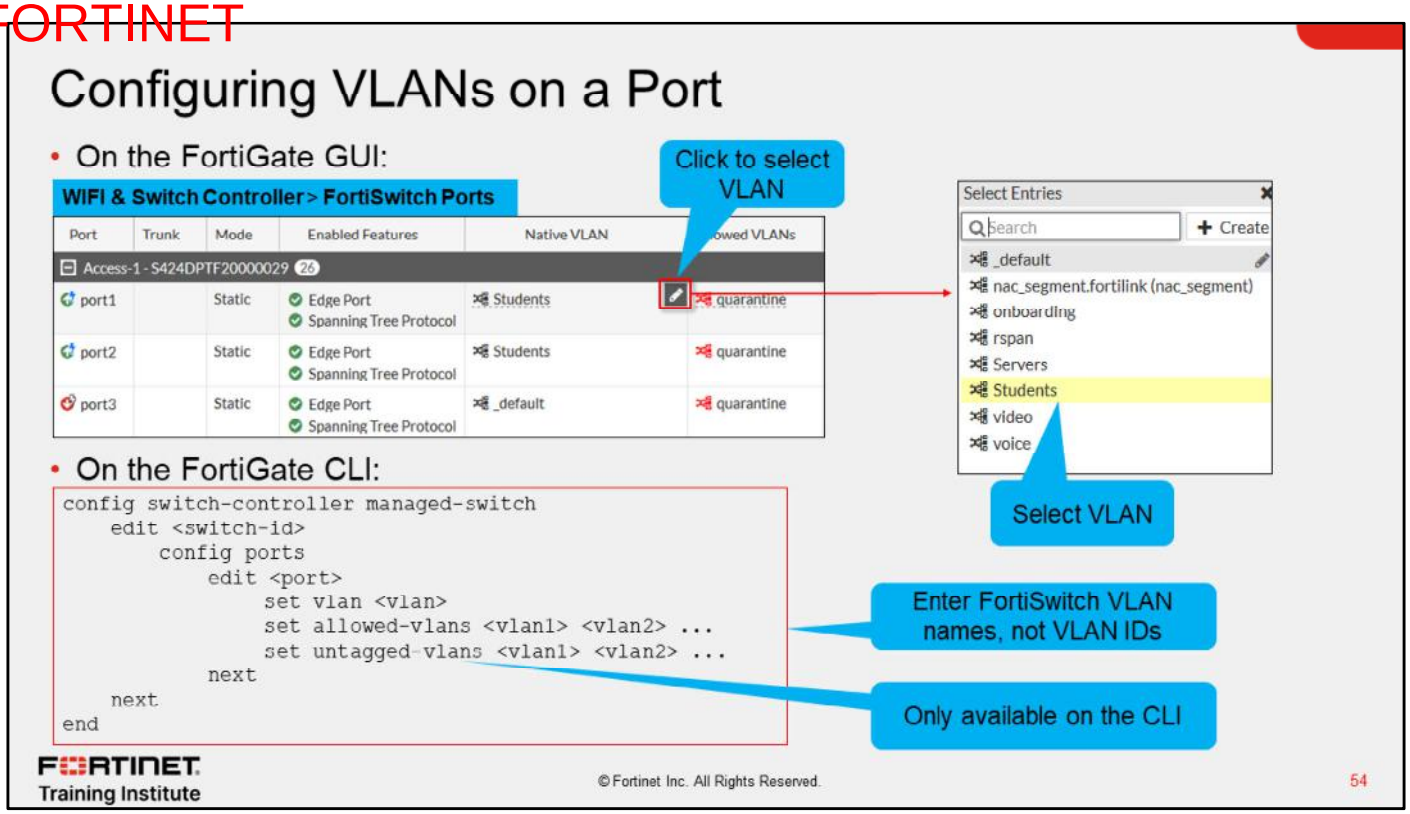
- Native VLAN: In most cases, this refers to the VLAN assigned to the endpoint. The native VLAN can be defined as the default VLAN for untagged ingress traffic. Because most endpoints send traffic without a VLAN tag, the endpoint traffic is placed in the VLAN defined as native VLAN. Frames for egress traffic matching the native VLAN are also sent untagged.

- Allowed VLANs: This defines the list of VLANs that are allowed on the port for both ingress and egress traffic, and for both tagged and untagged traffic. The native VLAN is implicitly allowed on the port, and therefore, you don't need to include it in the allowed VLANs list. For the port to accept incoming frames tagged with VLANs other than the native VLAN, the frames must be tagged with one of the VLANs defined in the allowed VLANs list. When there are no VLANs defined as untagged VLANs, the egress traffic for an allowed VLAN is tagged. The **Allowed VLANs** setting is important on ISLs, and in the FortiLink trunk, because the traffic forwarded between the switches, and between a switch and FortiGate, are usually tagged with multiple VLANs. You may also need to adjust the **Allowed VLANs** setting on ports connecting endpoints that send and expect to receive tagged traffic. This is the case for some IP phones or servers that leverage the use of VLAN tagging for their applications.

- Untagged VLANs: Usually, you don't have to configure this setting. However, some features like quarantine MAC or dynamic VLAN assignment, require it for the feature to work. This setting applies to egress traffic only, and defines a list of VLANs for which the egress traffic is sent untagged. For the setting to take effect, the untagged VLAN must also be a member of the allowed VLANs list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To edit the port's **Native VLAN** and **Allowed VLANs** settings on the GUI, browse to the **FortiSwitch Ports** page, and then hover over the corresponding column. A pencil icon appears. Click the pencil icon to display the list of VLANs that can be assigned. For the **Native VLAN** setting, you can select one VLAN only. For the **Allowed VLANs** setting, you can select multiple.

You can also use the CLI to configure the VLAN settings on a port by entering the CLI commands shown on the slide. Note that the `untagged-vlans` setting is available on the CLI only. In addition, note that when you specify a VLAN on the FortiGate GUI or CLI, you reference the name of the FortiSwitch VLAN and *not* its VLAN ID. Later, when FortiOS pushes the configuration to the switch, it assigns the corresponding VLAN ID to the switch port on FortiSwitchOS. FortiOS must perform this mapping because FortiSwitchOS references only VLAN IDs on its configuration, and not FortiSwitch VLAN names.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about VLANs is true?
   - ✓ A. They break down broadcast domains.
   - B. They cannot be extended across multiple switches.

2. Which statement about FortiSwitch VLANs is true?
   - A. They are used on FortiSwitch only.
   - ✓ B. They must be bound to a FortiLink interface.

3. Which VLAN setting controls the one or more VLAN IDs accepted on a port for both ingress and egress traffic?
   - A. Native VLAN
   - ✓ B. Allowed VLANs

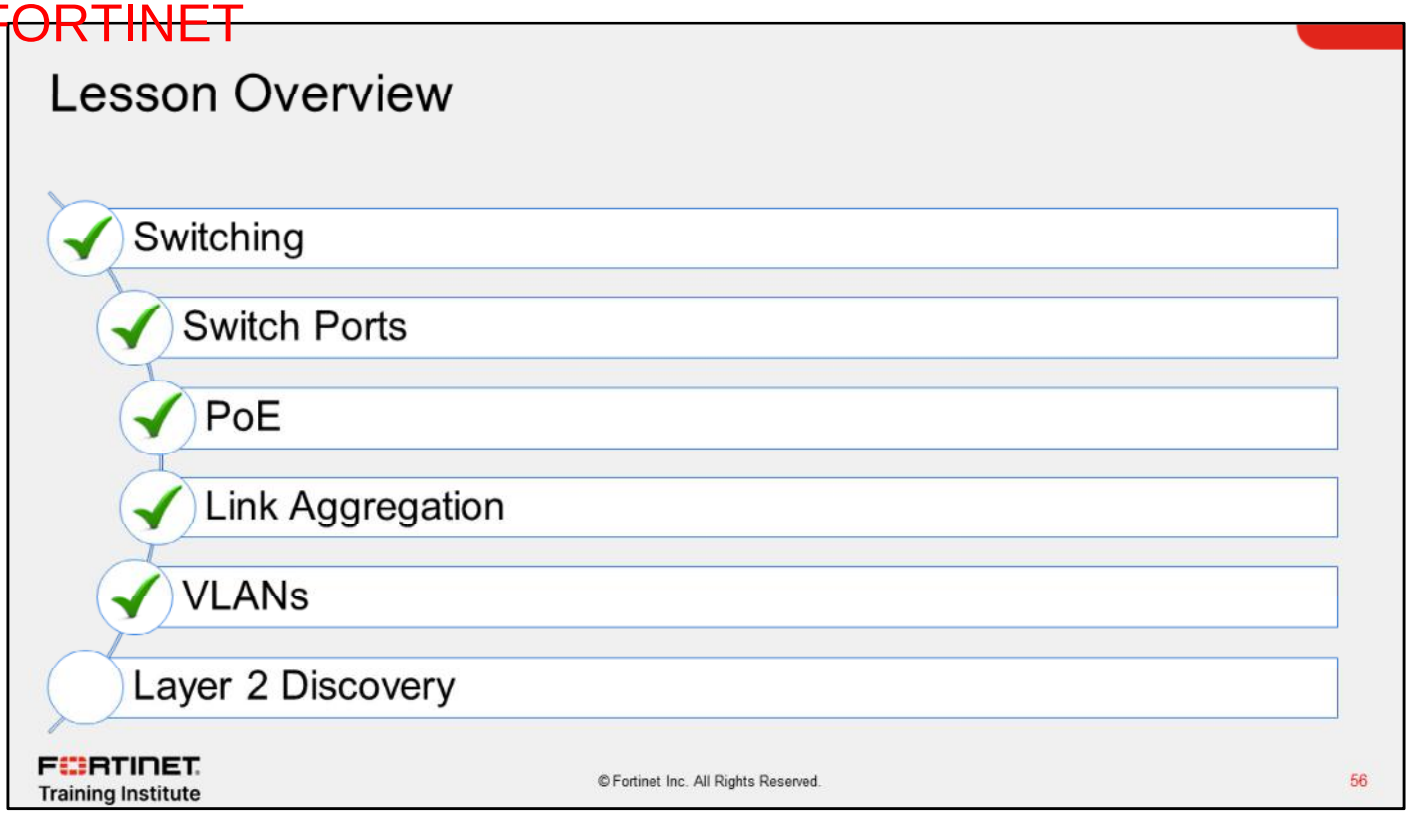
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

55

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

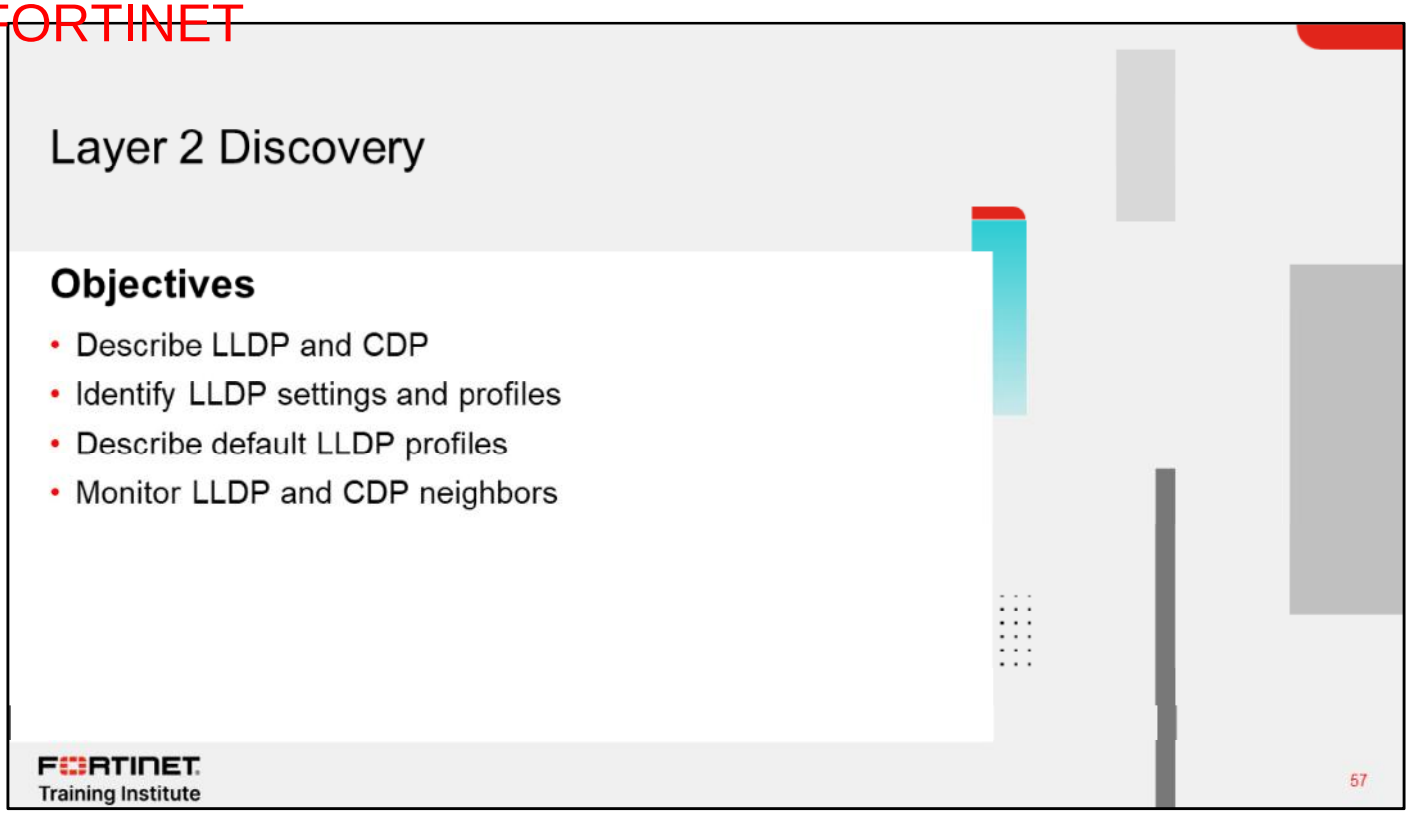


Good job! You now understand virtual LANs.

Now, you will learn about Layer 2 discovery protocols.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

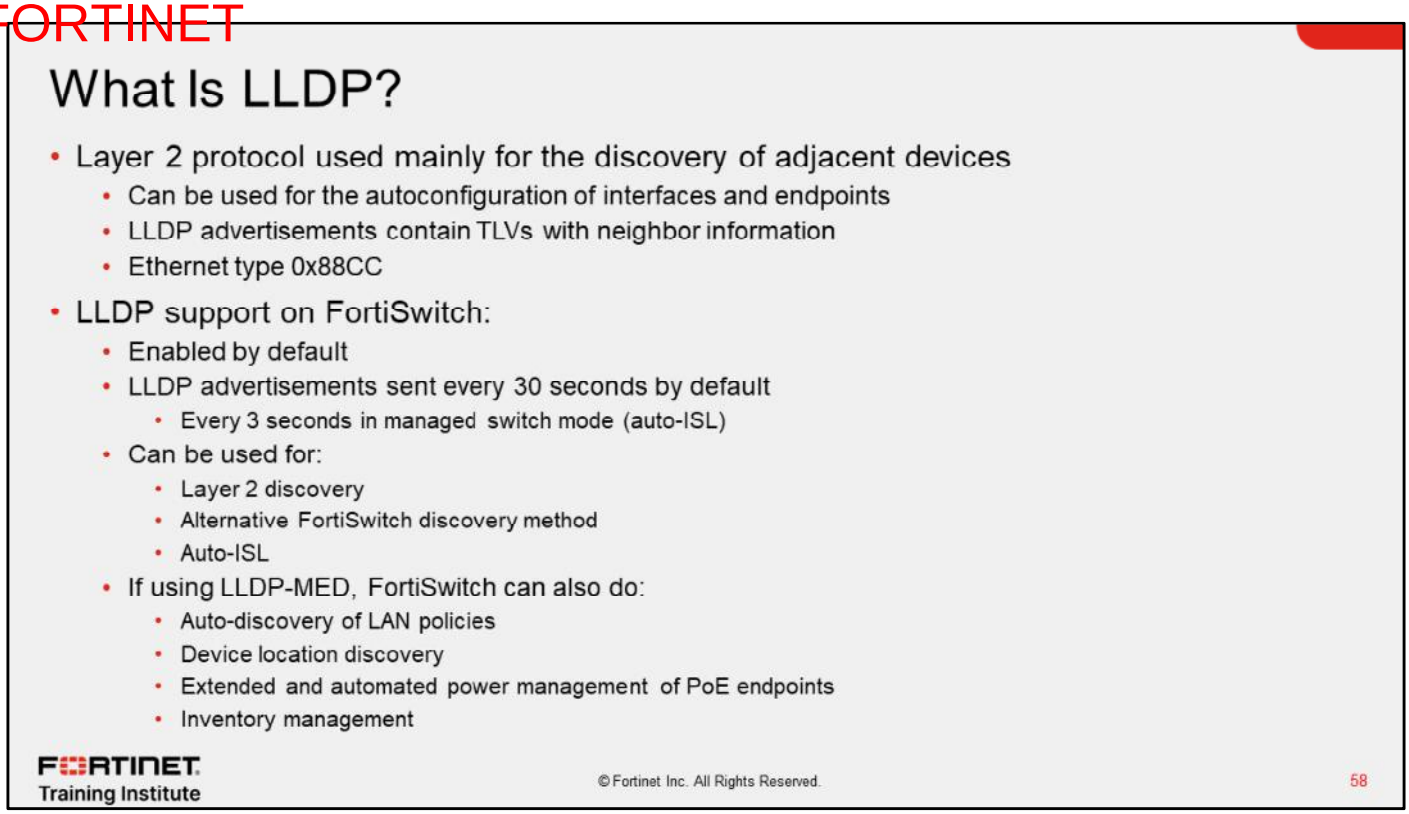


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in LLDP and CDP, you should be able to understand how FortiSwitch can discover adjacent devices, and how to display the neighbor information collected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



LLDP is an industry-standard Layer 2 protocol used for discovering adjacent devices in the LAN. LLDP-capable devices send LLDP advertisements periodically on connected ports to inform neighbors of their presence and capabilities. The neighbor information in an LLDP advertisement is contained in Type-Length-Value (TLV) structures. Neighbors then use TLVs mainly to maintain a list of discovered LLDP neighbors, but in some cases, to also perform tasks, such as the autoconfiguration of trunks, ports, and endpoints.

In FortiSwitch, LLDP is enabled out of the box, and LLDP advertisements are sent every 30 seconds by default. However, if the switch is operating in managed switch mode, the LLDP frames are sent every three seconds by default because of the auto-ISL feature. FortiSwitch uses LLDP for the following purposes:

- Layer 2 discovery: FortiSwitch maintains a list of discovered LLDP neighbors and their capabilities
- Alternative FortiSwitch discovery method: FortiGate discovers FortiSwitch devices based on their LLDP advertisements, instead of FortiLink discovery frames.
- Auto-ISL: FortiSwitch identifies an adjacent FortiSwitch or FortiGate from their LLDP advertisements, and then automatically forms a trunk for the adjacent device.

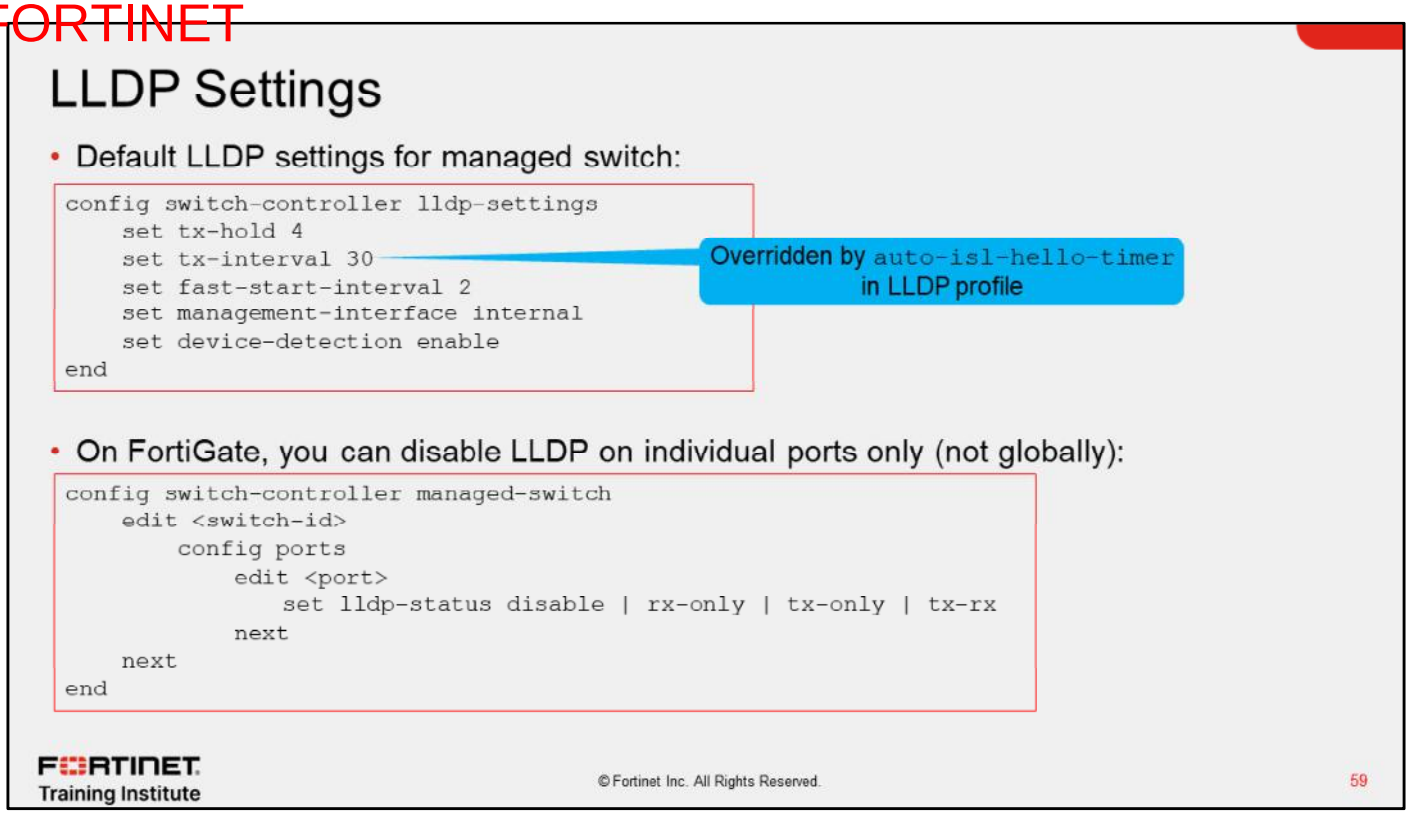
When using LLDP-Media Endpoint Discovery (LLDP-MED), which is an extension of LLDP, FortiSwitch also provides:

- Auto-discovery of LAN policies
- Device location discovery
- Extended and automated power management of PoE endpoints
- Inventory management

You will learn more about LLDP-MED in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



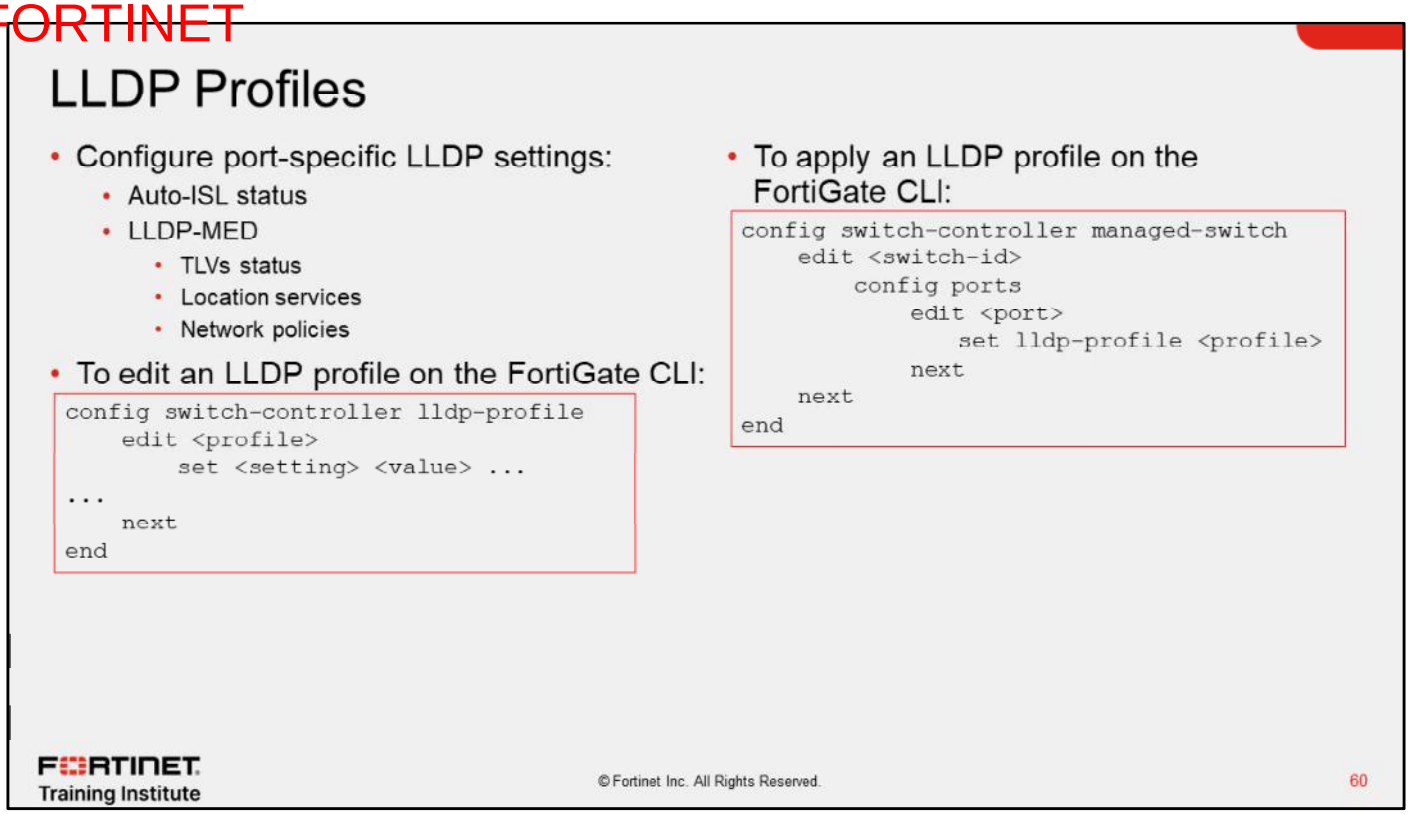
This slide shows the default LLDP settings:

- `tx-hold`: LLDP advertisements include a TTL TLV that defines how long the information contained in the LLDP frame should be stored on the receiver. The TTL value is calculated by multiplying the `tx-hold` value by the `tx-interval` value. On FortiSwitch, the default TTL is 120 seconds.
- `tx-interval`: Defines the frequency of the LLDP advertisements. In managed mode, each port is assigned the `default-auto-isl` LLDP profile, which has `auto-isl-hello-timer` set to 3 seconds. For this reason, in managed mode, the actual default interval is 3 seconds and not 30 seconds.
- `fast-start-interval`: Controls how often the FortiSwitch unit transmits the first four LLDP packets when a link comes up.
- `management-interface`: FortiSwitch uses the IP address of the interface selected here as the device management IP in LLDP advertisements.
- `device-detection`: When enabled, FortiSwitch forwards LLDP updates to FortiGate using CAPWAP to feed the FortiGate device detection daemon.

FortiOS does not support a CLI setting to globally disable LLDP on a managed switch. You can, however, disable LLDP on a per-port basis by disabling `lldp-status`, as shown on this slide. The default setting is to both send and receive LLDP frames (`tx-rx`), but you can also configure the setting to send LLDP frames only (`tx-only`) or receive LLDP frames only (`rx-only`).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



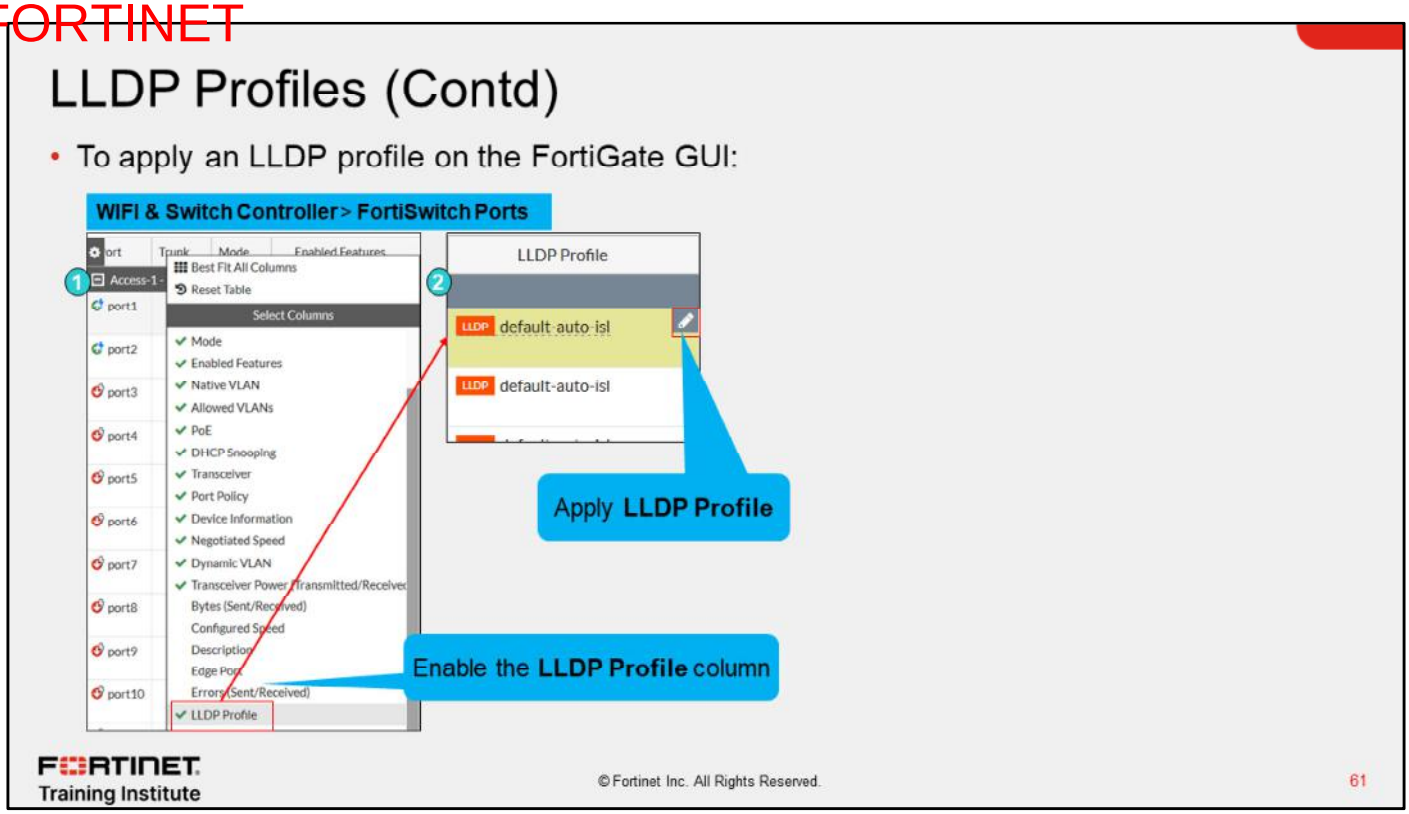
You use LLDP profiles to configure port-specific LLDP settings. For example, you can enable or disable auto-ISL, select the LLDP-MED TLVs you want to advertise, or configure the settings for LLDP-MED features, such as location services and network policies.

You can edit LLDP profiles on the FortiGate CLI only, but you can apply them using the FortiGate CLI or GUI. The slide shows how to configure and apply an LLDP profile on the CLI.

For information about available settings in an LLDP profile, see the *FortiSwitch—Managed Switch* document on `docs.fortinet.com`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can apply LLDP profiles on the **FortiSwitch Ports** page. First, enable the **LLDP Profile** column. Then, hover over the setting, click the pencil icon, and then select the LLDP profile in the list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Displaying LLDP Neighbors—Summary

- On the FortiGate CLI:

```
# diagnose switch-controller switch-info lldp neighbors-summary S548DF4K16000693
Vdom: root
Managed Switch : S548DF4K16000693       0

Capability codes:
       R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device
       W:WLAN Access Point, P:Repeater, S:Station, O:Other
MED type codes:
       Generic:Generic Endpoint (Class 1), Media:Media Endpoint (Class 2)
       Comms:Communications Endpoint (Class 3), Network:Network Connectivity Device

  Portname    Status   Device-name                    TTL   Capability  MED-type  Port-ID
  ----------  -------  -----------------------------  ----  ----------  --------  -------
  port1       Up       -                              -     -           -         -
  port2       Up       -                              -     -           -         -
...
  port51      Up       FG-601E-Active                 120   BR          -         04:d5:90:dc:35:34
  port52      Up       FG-601E-Backup                 120   BR          -         04:d5:90:dc:07:7c
  port53.1    Up       426ef                          120   BR          -         port27
  port53.2    Up       426ef                          120   BR          -         port28
  port53.3    Up       524d                           120   BR          -         port25
  port53.4    Up       524d                           120   BR          -         port26
```

FortiGate port MAC address

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

62

You must use the FortiGate CLI to display the LLDP neighbors discovered by your stack of switches. This slide shows the command you can run to display a summary of the information learned from LLDP on each port. Usually, you will be interested in looking at the `Device-name` and `Port-ID` columns, which enables you to quickly identify the adjacent neighbor and port.

Note that, in the example, FortiGate advertises the MAC address of its port as the port ID. This happens when the FortiGate port does not have an alias configured. If an alias is set, FortiGate then advertises the alias as the port ID instead.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying LLDP Neighbors—Detail

- On the FortiGate CLI:

```
# diagnose switch-controller switch-info lldp neighbors-detail S424DPTF20000027 port23
Vdom: root
Managed Switch : S424DPTF20000027       0

Capability codes:
        R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device
        W:WLAN Access Point, P:Repeater, S:Station, O:Other

MED TLV Capability codes:
        C:Capabilities, P:Network Policies, L:Location, S:MDI PSE
        D:MDI PD, I:Inventory

_____________________________________________________________
Neighbor learned on port port23 by LLDP protocol
Last change 328873 seconds ago
Last packet received 2 seconds ago

Chassis ID: 00:50:56:96:b1:a8 (mac)
System Name: FortiGate-1.trainingAD.training.lab
System Description:
FortiGate-VM64 v7.2.1,build1254,220803 (GA.F)
...
```

FortiOS version

FORTINET Training Institute

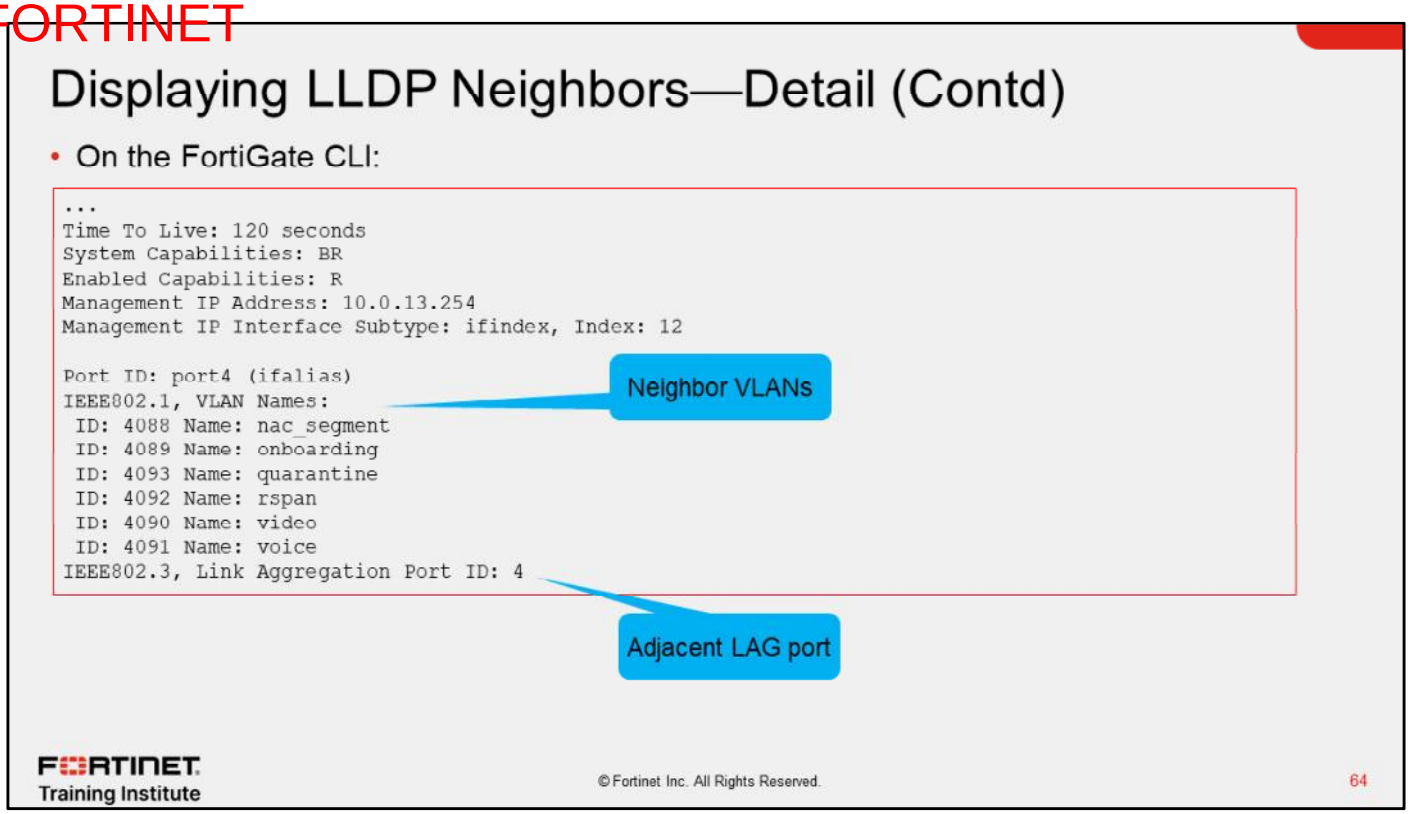
© Fortinet Inc. All Rights Reserved.

63

Use the command shown on this slide to display all information learned from LLDP on a specific port. The output was cut to fit on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

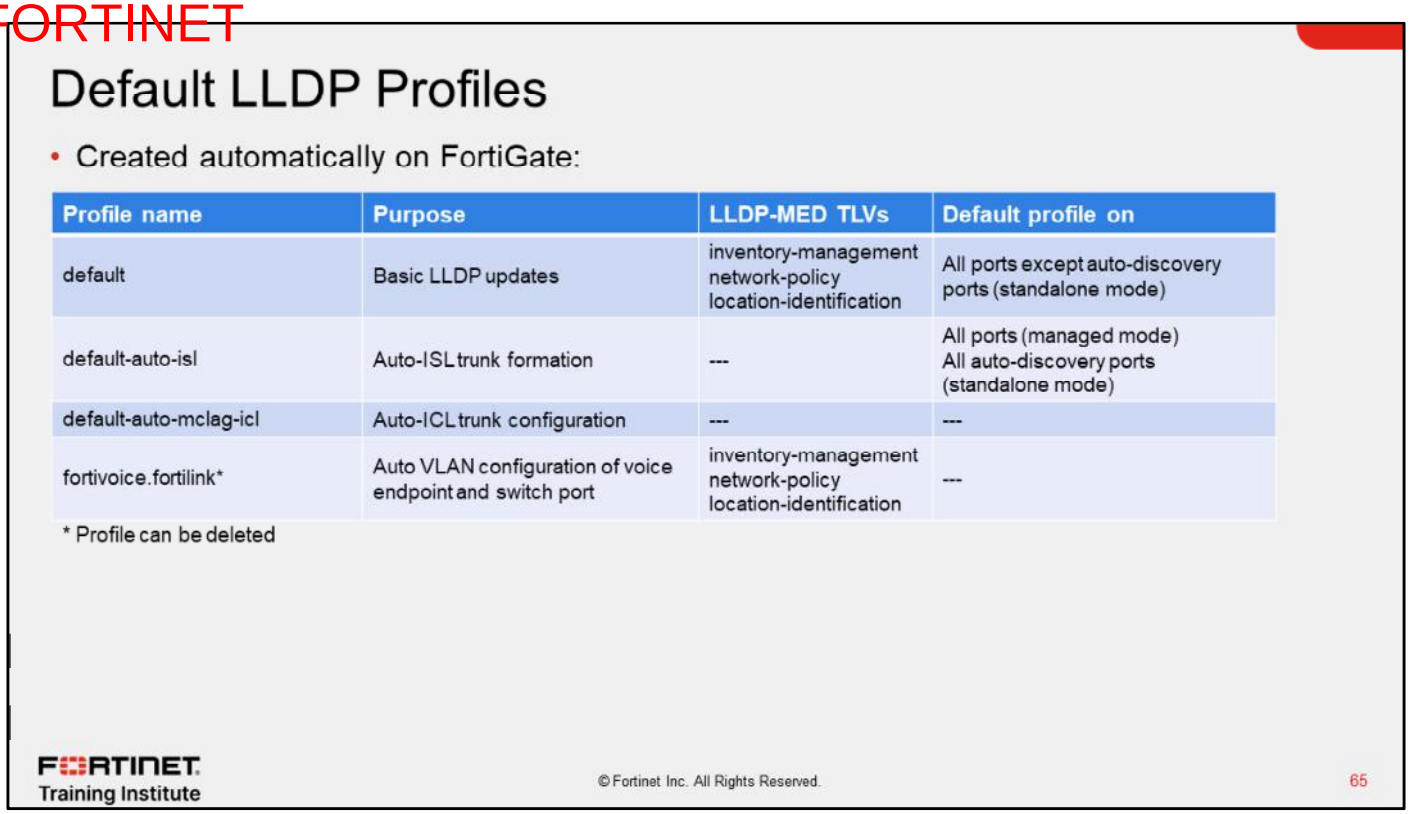


This slide shows the remaining portion of the LLDP detailed output. Note that the VLANs present in the neighbor are also included in the output. In addition, because the neighbor is connected over a trunk, the output also indicates the port ID (port4) of the port on the adjacent device used for the LAG.

Note that the information displayed for each neighbor depends on the information it advertises. Therefore, expect the information to vary across different device types and vendors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The table on this slide shows the LLDP profiles that are created by default on FortiSwitch, and their intended use.

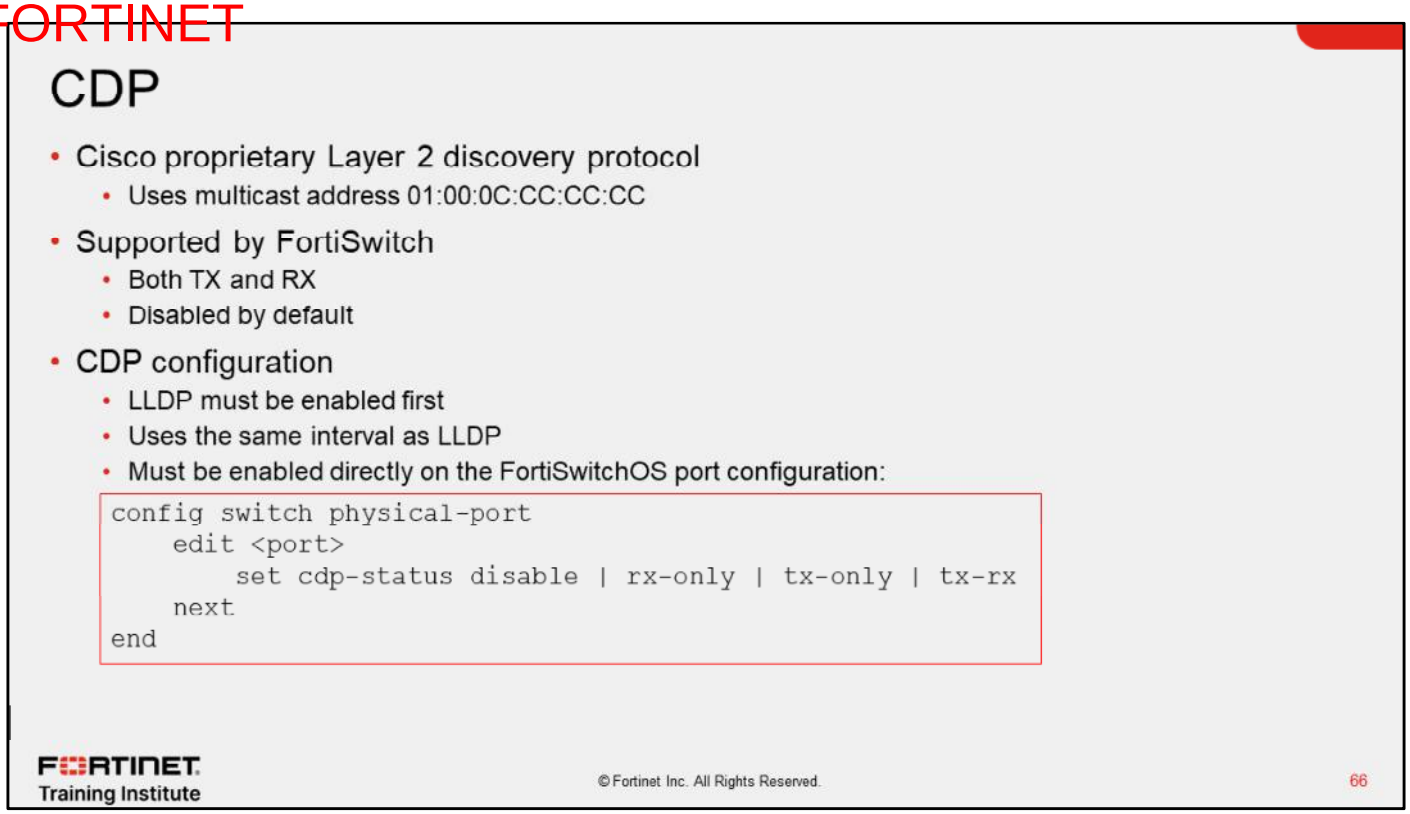
In FortiSwitch managed switch mode, all ports are assigned the `default-auto-isl` profile by default. The same profile is also used in standalone mode on auto-discovery ports only. All other ports on a standalone mode FortiSwitch are assigned the `default` profile.

The other two profiles, `default-auto-mclag-icl` and `fortivoice.fortilink`, are not enabled by default on any ports. However, the administrator may want to use them to automatically configure MCLAG ICL trunks between two switches forming an MCLAG peer group, and to automatically configure VLAN settings on voice endpoints and the FortiSwitch ports they are connected to, respectively.

Note you can't delete any of the default LLDP profiles, except `fortivoice.fortilink`. You can, however, edit all of them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



CDP is a proprietary protocol developed by Cisco for discovering adjacent devices in a LAN. FortiSwitch supports receiving and processing of CDP advertisements, as well as their transmission.

CDP is disabled on FortiSwitch by default. You enable CDP on a per-port basis. Because FortiOS does not support a CLI setting to enable CDP, you must either apply the configuration directly on the switch or use the custom command tool available on FortiGate.

This slide shows the CLI commands you must run on FortiSwitchOS to enable CDP on a port. As with LLDP, you can select whether you want to only transmit CDP advertisements, only receive CDP advertisements, or both transmit and receive CDP advertisements.

Note that CDP only works if you previously enabled LLDP on the port. In addition, CDP advertisements are transmitted at the same interval configured for LLDP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying CDP Neighbors—Detail

- On the FortiGate CLI:

```
# diagnose switch-controller switch-info lldp neighbors-detail
Vdom: root
Managed Switch : S224EPTF19005928       0

Capability codes:
        R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device
        W:WLAN Access Point, P:Repeater, S:Station, O:Other

MED TLV Capability codes:
        C:Capabilities, P:Network Policies, L:Location, S:MDI PSE
        D:MDI PD, I:Inventory

_____________________________________________________________
Neighbor learned on port port5 by CDPv2 protocol
Last packet received 10 seconds ago

Chassis ID: 3560CX-port11 (local)
System Name: 3560CX-port11
System Description:
cisco WS-C3560CX-8PT-S running on
...
```

FORTINET Training Institute

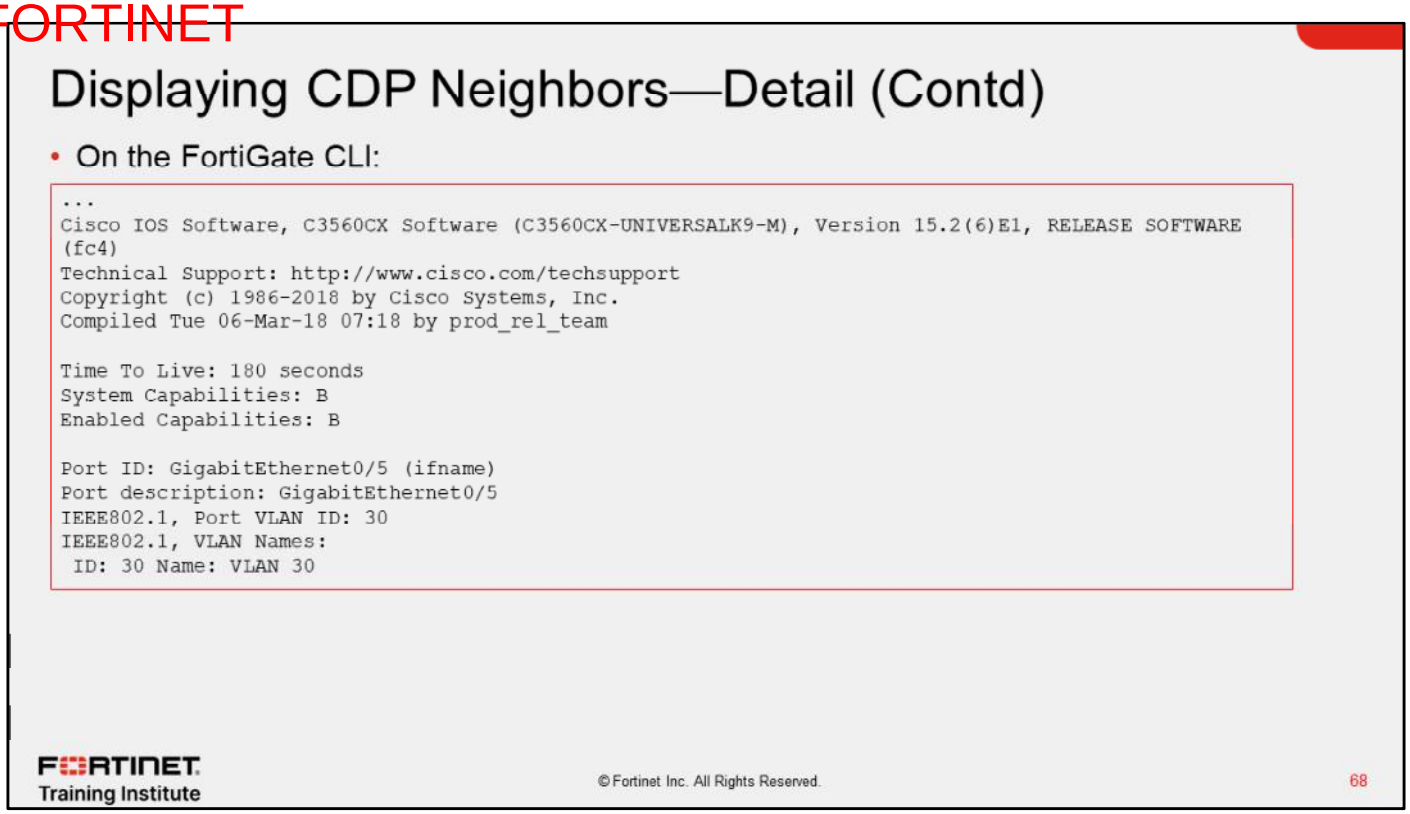
© Fortinet Inc. All Rights Reserved.

67

You use the same command for LLDP detailed neighbor information to display CDP neighbors. The example shown on this slide was cut to fit on the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the remaining portion of the CDP neighbor detailed output.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about LLDP is true?
   - A. LLDP is disabled by default on FortiSwitch.
   - ✓ B. TLVs in LLDP advertisements contain the neighbor information.

2. What is the default interval for LLDP advertisements when FortiSwitch is in managed mode?
   - ✓ A. 3 seconds
   - B. 30 seconds

3. Which statement about CDP is true?
   - A. CDP is enabled by default on FortiSwitch.
   - ✓ B. LLDP must be enabled for CDP to work.

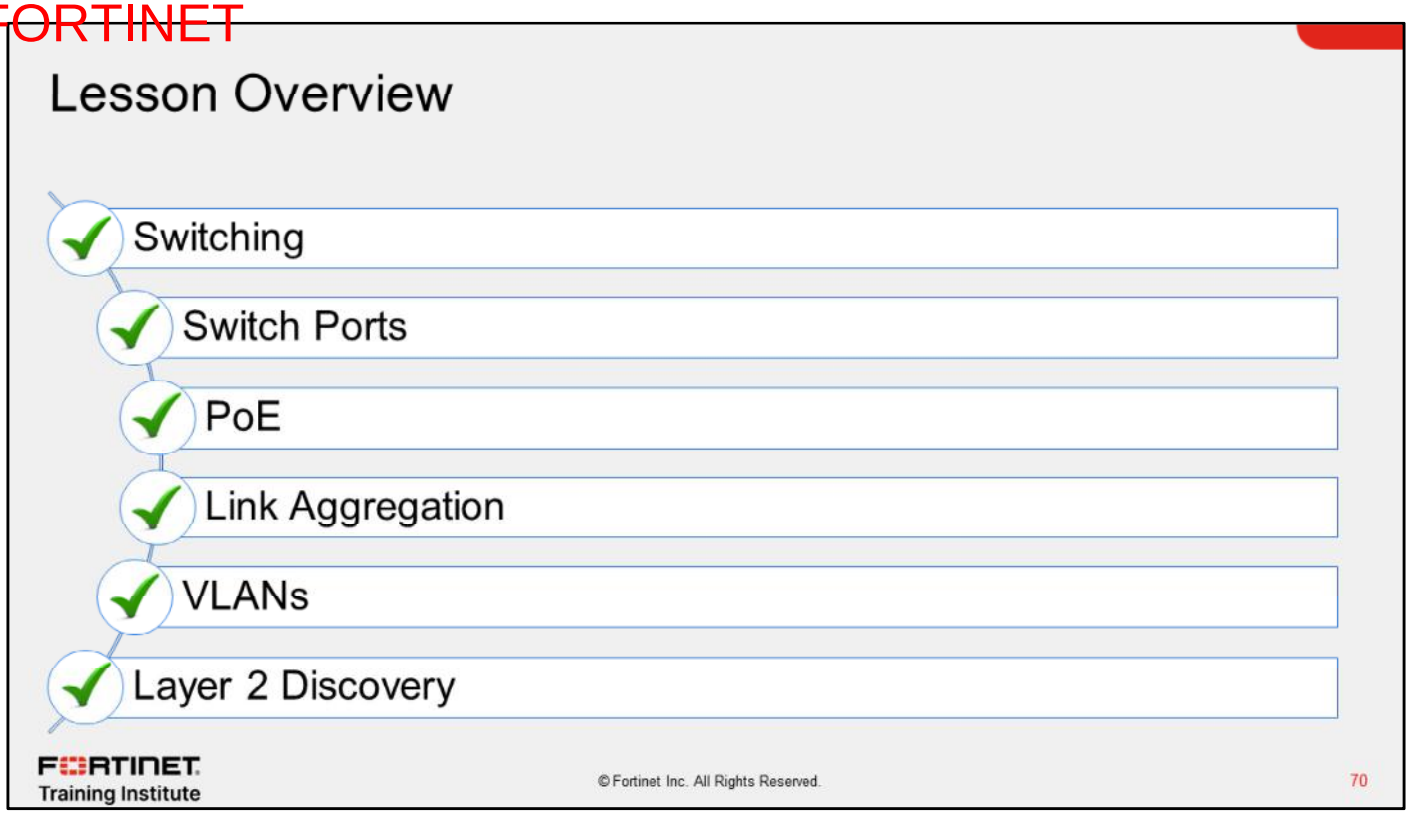
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

69

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

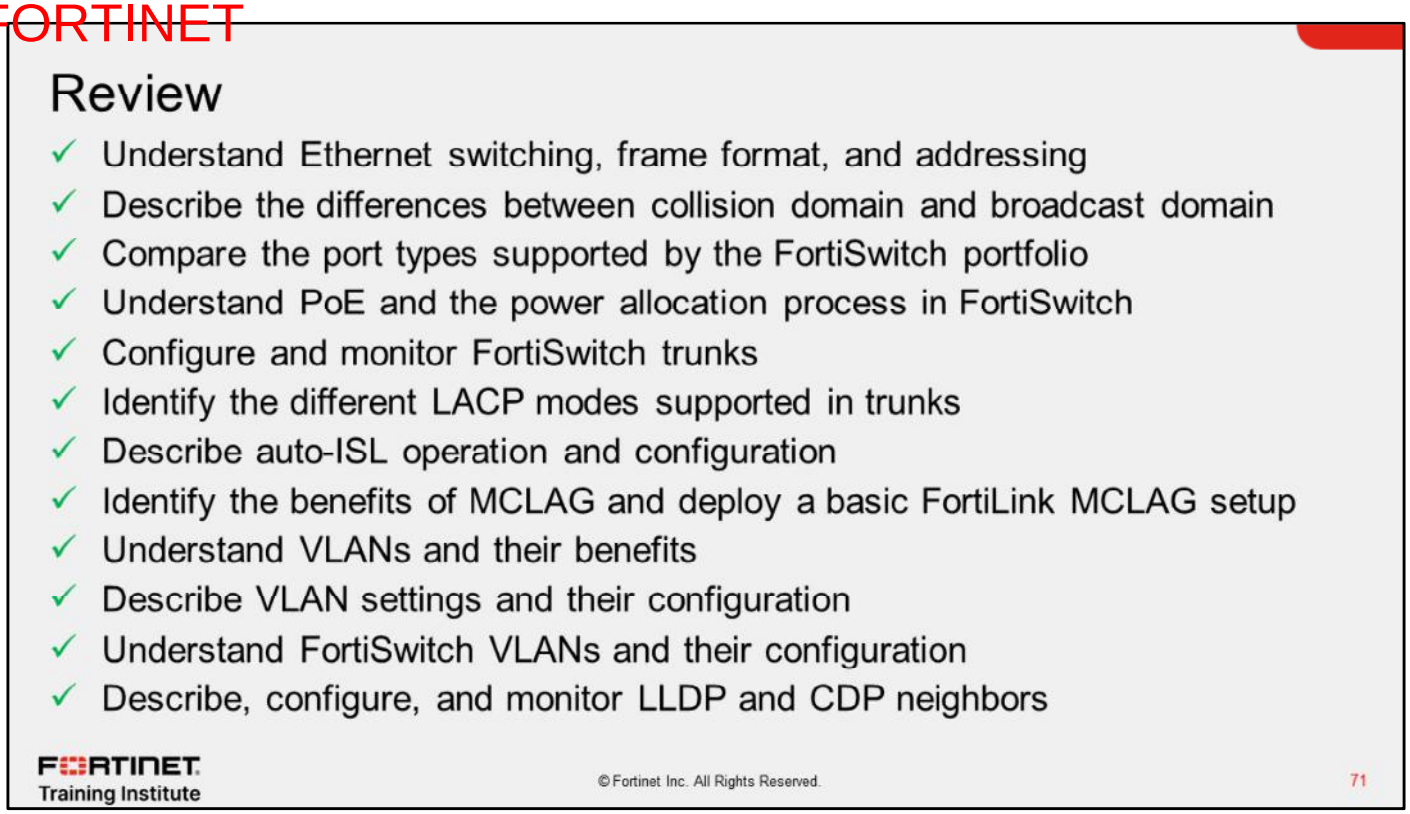


Good job! You now understand Layer 2 discovery.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

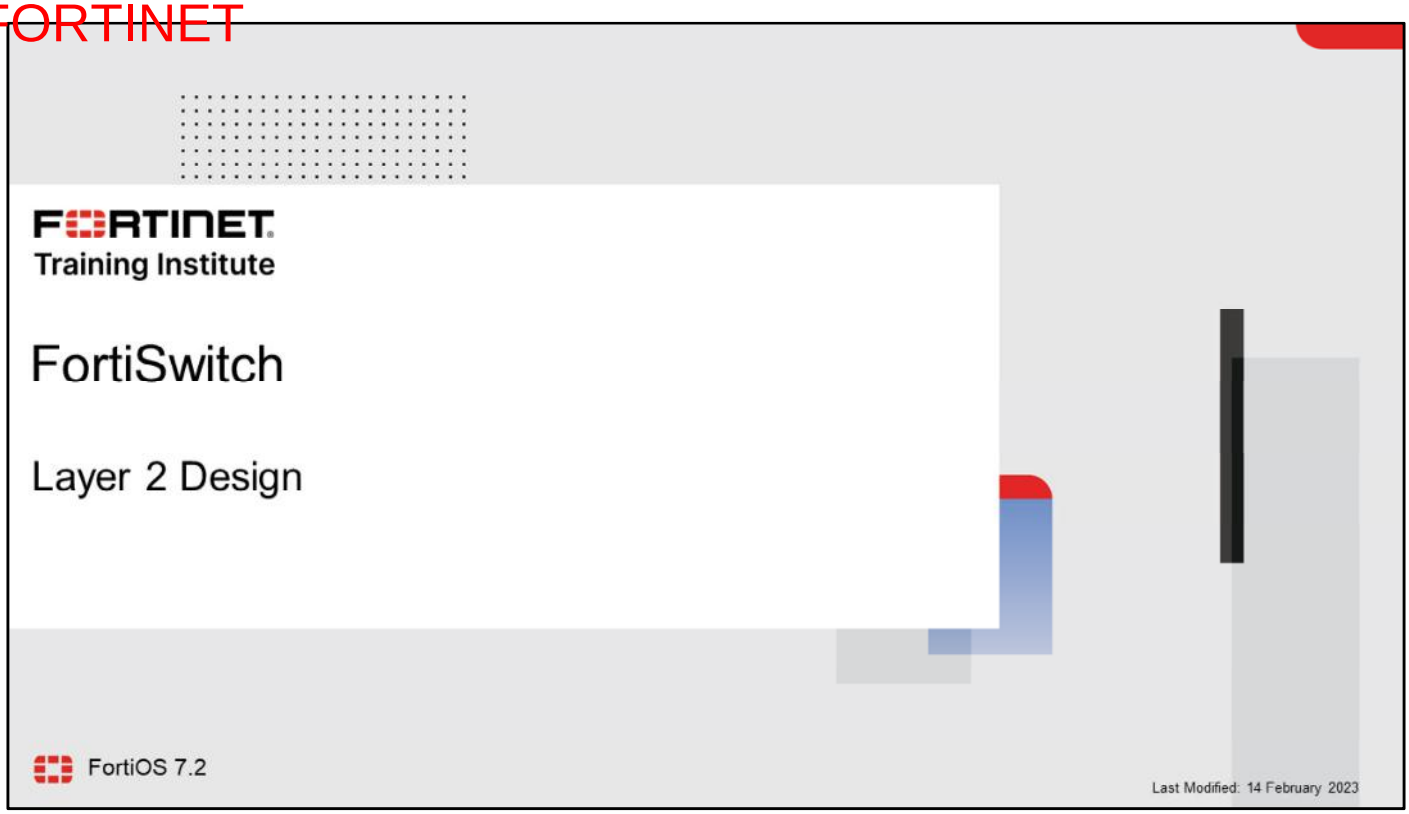


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about Ethernet switching fundamentals, and how to configure basic Layer 2 features on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

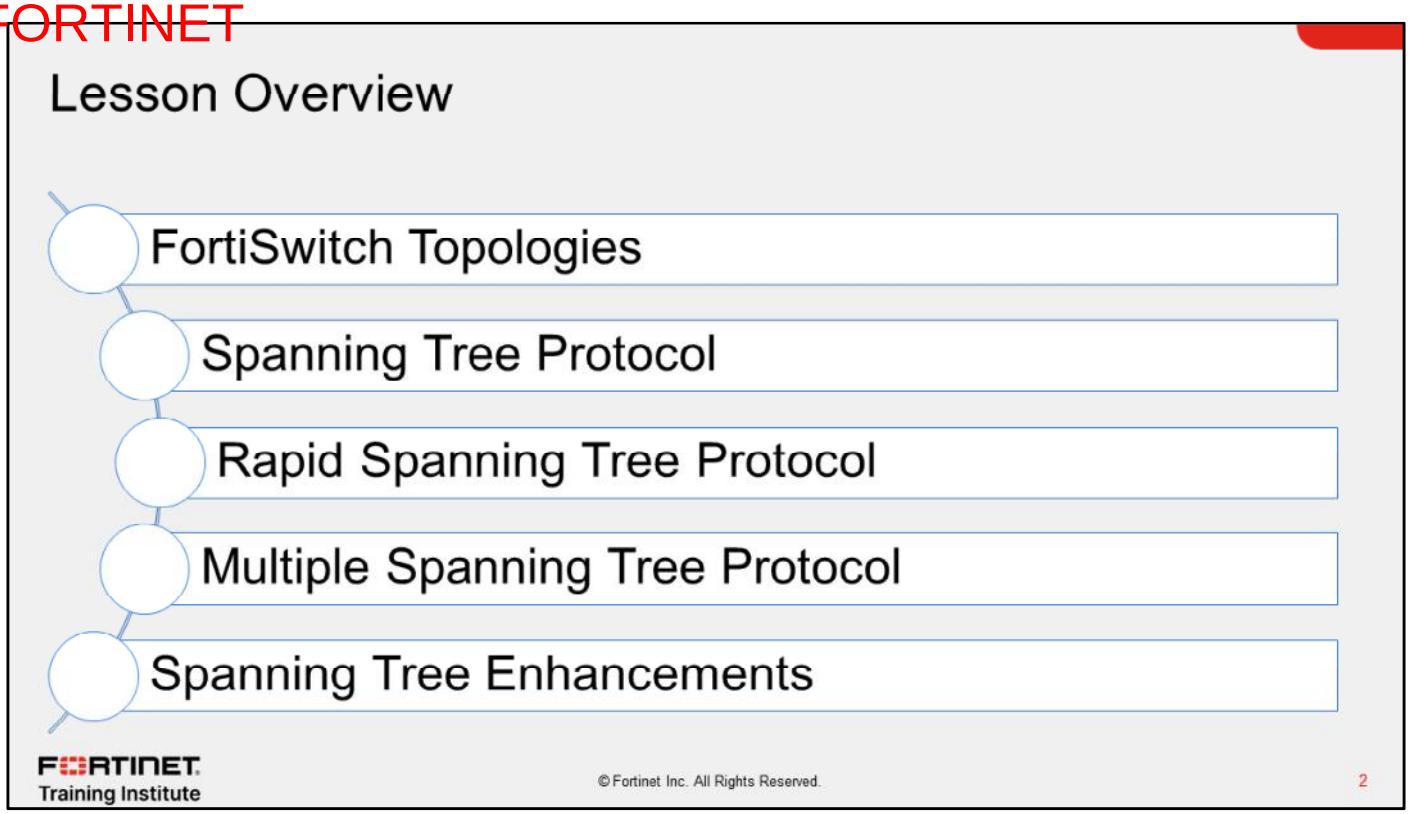
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the most common FortiSwitch topologies, as well as the different loop prevention protocols and methods available on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

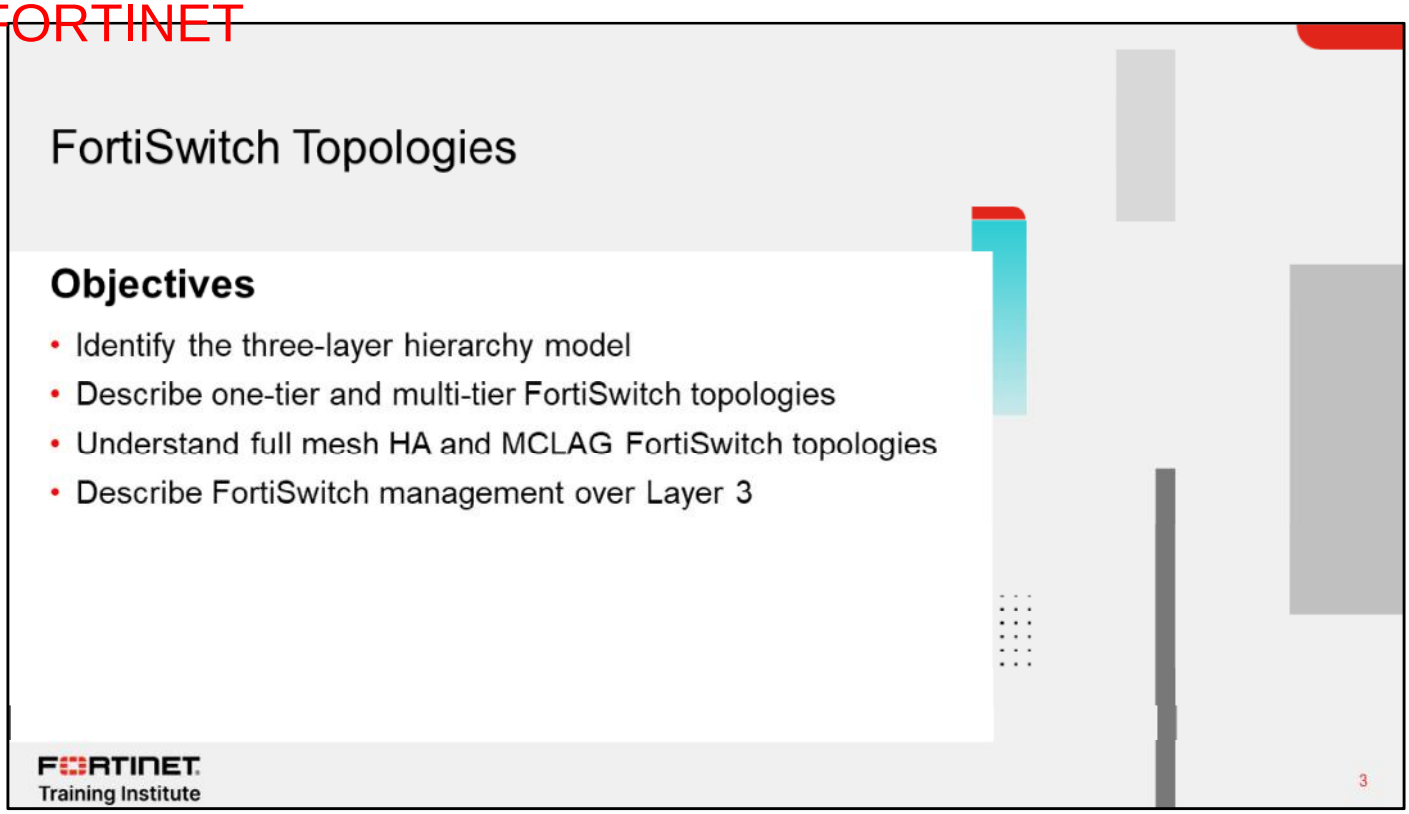
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

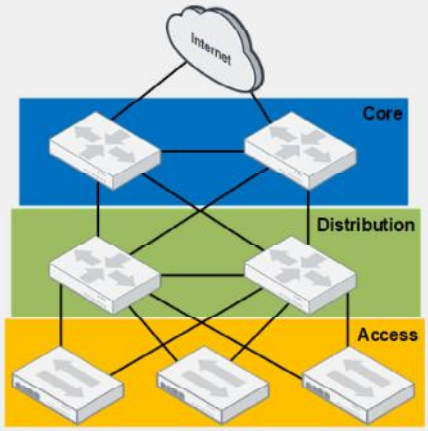
By demonstrating competence in FortiSwitch topologies, you should be able to identify the topology that best suits your network design requirements.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

The Three-Layer Hierarchy Model

- Widely known network design model
- Core layer
  - Network backbone
  - High-speed is crucial
  - Redundancy and fault tolerance
  - No resource-intensive tasks
  - Uses Layer 2 or Layer 3 devices
- Distribution layer
  - Traffic aggregation
  - Inter-VLAN routing, packet inspection, and filtering
  - Redundancy and fault tolerance is recommended
  - Uses Layer 2 or Layer 3 devices
- Access layer
  - Provides connectivity and power to endpoints
  - VLAN segmentation, authentication, NAC, and QoS
  - Mainly composed of high-density port switches



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

When it comes to network design, network administrators often refer to the core, distribution, and access layers described in the widely known and adopted three-layer hierarchy model. The supported FortiSwitch network topologies also refer to these layers when describing the roles of FortiGate and FortiSwitch devices.

The three-layer hierarchy model can be used as a guideline for designing reliable, scalable, and cost-effective networks. It divides the network into the following layers:

- Core: Also known as the backbone, this layer provides reliable high-speed transport between the WAN, the internet, and the distribution layer. The most important consideration is speed. For this reason, devices in this layer should perform mostly switching; however, routing may also be implemented. Resource-intensive tasks, such as security inspection or QoS classification, should be avoided. Redundancy and fault tolerance are highly recommended. Layer 2 or Layer 3 devices can be used in this layer.

- Distribution: Also known as the smart layer, this layer aggregates traffic from the access layer switches and forwards it to the core devices. Inter-VLAN routing, security inspection, packet filtering, and other packet manipulation tasks should take place here. Redundancy and fault tolerance are recommended. Layer 2 or Layer 3 devices can be used in this layer.

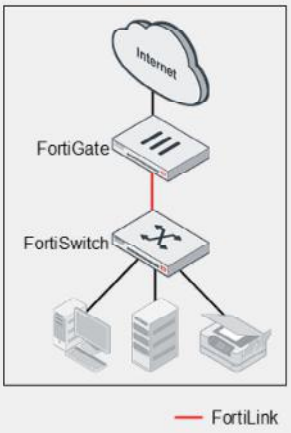
- Access: This is where you connect the endpoints: workstations, phones, access points, servers, and so on. The access layer is usually composed of Layer 2 switches and provides network connectivity to endpoints. When using power over Ethernet (PoE), the access layer also delivers power to personal devices (PDs). In addition, the access layer often performs VLAN segmentation, device authentication, network access control (NAC), and QoS classification. Access layer switches usually have a high-density port configuration to reduce per-port costs. Usually, redundancy and fault tolerance are not a requirement.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Single FortiGate and Single FortiSwitch

- One FortiGate controlling one FortiSwitch
- FortiLink can be:
  - Physical port
    - No LAG support (FortiOS 6.2 and lower)
  - LAG
    - Usually offers best scalability and throughput
  - Switch interface (hardware or software-based)
    - Limited scalability and throughput
- Collapsed core design
  - Two-layer hierarchy
  - Reduces network costs
  - Distribution and core functions merged
    - Performed by FortiGate
  - FortiSwitch acts as an access layer switch



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

The most basic FortiSwitch topology involves a single FortiGate controlling one FortiSwitch. You can configure the FortiLink interface as a single physical port, a link aggregation (LAG) with one or more LAG members, or a hardware or software-based switch interface.

Most of the time, it's better to use a LAG because it enables you to easily scale without having to reconfigure the FortiLink interface, while offering the best throughput. You can also use a physical port for your FortiLink interface, but this option really makes sense if your FortiGate doesn't support LAG. However, starting FortiOS 6.4, all FortiGate devices support LAGs, so in that case, using a LAG with a single member interface is a better option.

A third option is to configure the FortiLink interface to use hardware-based or software-based switch interfaces. This setup is useful when you want to connect all your switches directly to FortiGate, instead of stacking them. However, it's only recommended for small networks, where scalability and throughput are not expected to grow over time. That is, for every FortiSwitch you add to the network, you must have a port on FortiGate. In addition, when you connect multiple switches directly to FortiGate, intra-VLAN traffic from endpoints connected to different switches is also processed by FortiGate, which can lead to a bottleneck especially, if a software-based switch interface is used.

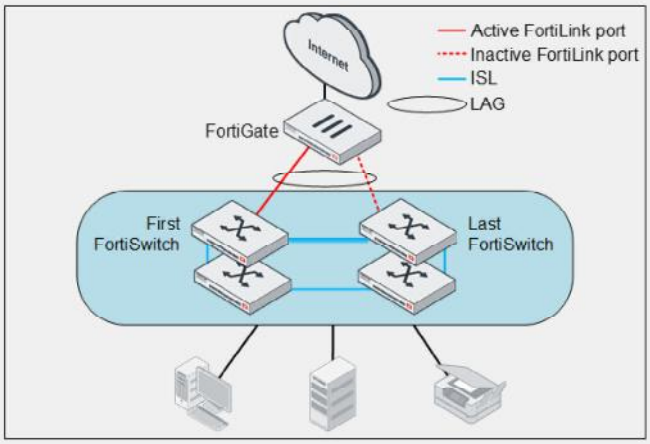
The topology on this slide shows FortiSwitch as the access layer switch and FortiGate as both the distribution and core device. When the same device performs the core and distribution tasks, the layer in which this group of devices operates is called a collapsed core. Under this design, the network becomes a two-layer hierarchy topology. To reduce costs, you can use this topology in smaller networks that you don't expect will have a significant increase in traffic over time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Single FortiGate and FortiSwitch Stack

- Group of switches connected using ISLs
  - Add switches as network grows
- Ring stack topology provides FortiLink redundancy
  - FortiLink interface must be a LAG
    - FortiLink split interface must be enabled
  - If first FortiSwitch fails, inactive FortiLink is used
    - Inactive FortiLink: port status is down (no link)
- Collapsed core



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

As your network grows, you can add more switches to the single FortiGate and single FortiSwitch topology to form a FortiSwitch stack.

The additional switches can be connected using inter-switch links (ISLs). You keep the first switch connected to the FortiLink interface, and optionally, you also connect the last switch to the FortiLink interface to form a ring. When you use a ring connection to connect your switch stack directly to FortiGate, you must configure the FortiLink interface as a LAG. You must also enable the FortiLink split interface setting to instruct FortiGate to keep only one FortiLink port active (link up) at a time. Other FortiLink port members are inactive (link down). If the active port goes down, one of the inactive ports becomes active. When you enable FortiLink split interface, management and user traffic is not affected when two or more FortiLink port members connect to two different switches that aren't configured as multi-chassis link aggregation (MCLAG) peers, which is the case in this topology.

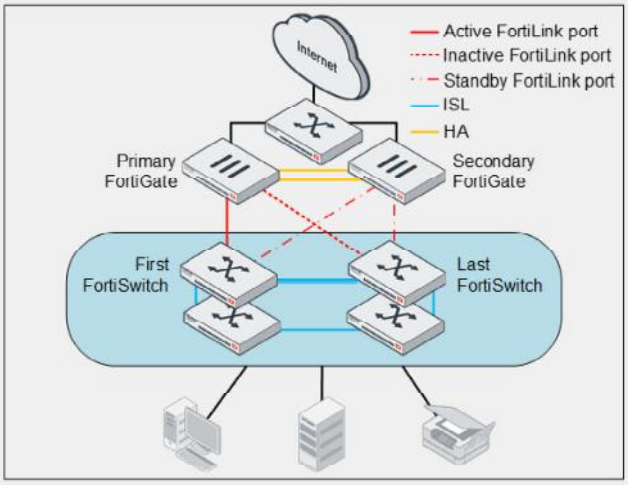
Using a ring to connect your FortiSwitch stack, provides you with redundancy for the FortiLink connection. If the first switch is lost, the standby FortiLink connection becomes active, so the rest of the switches can continue communicating with FortiGate through the last switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate HA and FortiSwitch Stack

- Both A-P and A-A modes supported (FGCP)
  - Only the FortiGate primary controls the stack
  - FortiGate secondary takes over stack on HA failover
- Connect secondary FortiGate to first and last switch
- FortiLink split interface is enabled (no MCLAG support)
  - Doesn't affect ports on secondary FortiGate
  - Active FortiLink port on primary FortiGate is used for management and user traffic
    - Secondary link on primary FortiGate is inactive (link down)
- Collapsed core



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

You can also manage a FortiSwitch stack from a FortiGate HA cluster. Both FortiGate Clustering Protocol (FGCP) active-passive (A-P) and active-active (A-A) modes are supported.

When you add a secondary FortiGate to the topology, you must also connect the first and last FortiSwitch devices to that secondary FortiGate. Note that the primary FortiGate is *the only device* used for switch management. That is, the secondary FortiGate can be used for processing user traffic—if A-A mode is enabled—but only the primary FortiGate controls the FortiSwitch stack.

FortiLink split interface is enabled. As a result, out of the four FortiLink ports, only one port—the active FortiLink port on the primary FortiGate—is used for switch management. The active FortiLink port on the primary FortiGate is also used for processing user traffic. The other FortiLink ports on the primary FortiGate are inactive (link down). Also, the ports on the secondary FortiGate—the standby FortiLink ports in the topology—are not affected by the FortiLink split interface setting. That is, the ports on the secondary FortiGate remain up (link up), and on standby for switch management. On an HA failover, the secondary FortiGate takes over the cluster and the FortiSwitch stack management, and like the former primary FortiGate, it will have only one active FortiLink port, which is used for both switch management and user traffic.

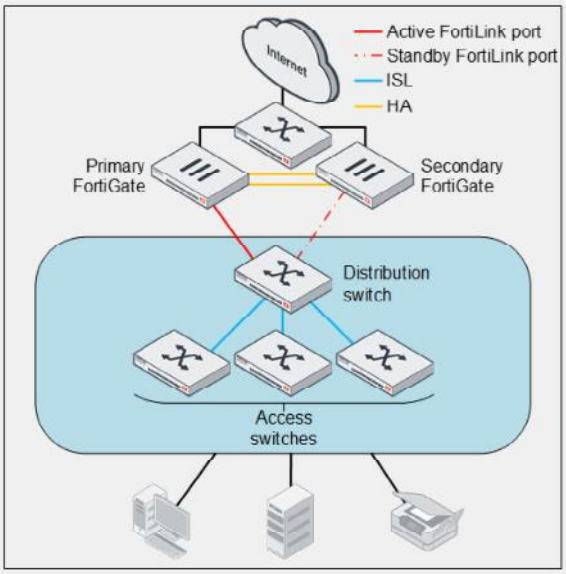
The setup shown on this slide makes sense only when MCLAG is not supported by FortiSwitch—most FortiSwitch models support MCLAG. Otherwise, it's better to use MCLAG and disable FortiLink split interface for better throughput. Also, the topology on this slide shows a single switch that connects FortiGate to the internet. However, you can also use a pair of FortiSwitch devices acting as an MCLAG peer group for redundancy purposes. You will learn more about setting up MCLAG and MCLAG topologies in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate HA and Two-Tier FortiSwitch Stack

- More hierarchical design
  - No collapsed core
    - FortiGate is the core device
    - Separate switches for distribution and access (two-tier)
- Distribution switch
  - Aggregates traffic from access layer switches
    - Choose model with enough switching capacity
  - Mainly forwards traffic (no smart tasks)
  - Single point of failure



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

Following a more hierarchical network design, you can separate the collapsed core layer into distinctive core and distribution layers by deploying a two-tier FortiSwitch stack topology.

The access switches connect to a distribution switch that aggregates the traffic from endpoints and forwards it to FortiGate for security inspection, inter-VLAN routing, and other security-related tasks. The distribution switch in this topology, and any topology using managed switches, does not perform the smart tasks described in the three-layer hierarchical model. These tasks are performed by FortiGate, which acts as the core device.

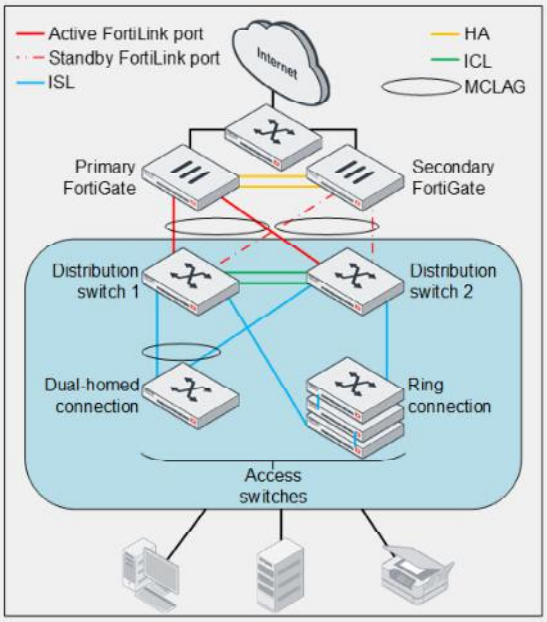
The distribution switch works more like an *aggregation switch* because it mainly forwards traffic between access switches and FortiGate. For this reason, you should select a FortiSwitch model that can handle the network bandwidth requirements of the aggregated traffic. The existence of one distribution switch only results in a single point of failure in the switch stack. You can achieve redundancy by adding another distribution switch and using MCLAG as shown in the next slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate HA and One-Tier MCLAG

- Use MCLAG on distribution switches to:
  - Eliminate single point of failure in LAN
    - LAG members terminate on different switches
  - Increase throughput
  - Use dual-homed connection on access switches
- Disable FortiLink split interface on FortiGate
  - Both LAG members on primary FortiGate are active
- Use at least two ICL links (redundancy)
- `mclag-stp-aware` on distribution switches must be enabled (default = `enabled`)
  - Runs STP on MCLAG ICL links
- Access switch connection
  - Dual-homed
    - Redundancy, higher performance
  - Ring
    - Redundancy (STP)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

By adding a second distribution FortiSwitch and configuring MCLAG, you can achieve redundancy across your LAN. You configure both distribution switches as MCLAG peers, so the FortiGate HA cluster and access switches form LAGs terminating on both distribution switches. The result is that losing a distribution switch, a FortiGate device, or an uplink on the access switch won't result in permanent service disruption. Instead, the traffic continues to be forwarded through the redundant paths. Also, the use of LAGs on FortiGate and access switches results in more throughput across the network.

On FortiGate, make sure FortiLink split interface is disabled after you finish setting up MCLAG on the distribution switches. This ensures that both LAG members on the primary FortiGate are active. On the distribution switches, it's recommended to use at least two ICL links for redundancy. In addition, `mclag-stp-aware` must be enabled—it's enabled by default. When `mclag-stp-aware` is enabled, the switch runs Spanning Tree Protocol (STP; IEEE 802.1D) on MCLAG ICL links to detect loops caused by non-ICL links between MCLAG peers. You will learn more about STP in this lesson.

You can use a dual-homed connection for an access switch, or a ring topology for multiple access switches. In a dual-homed connection, you use two uplinks, each connected to a different distribution switch peer. If using MCLAG, the uplinks in a dual-homed connection operate as a LAG. In a ring connection, you stack multiple switches, and then connect only the first and last switches in the stack to different distribution switch peers. When compared to a dual-home connection, a ring connection requires fewer uplinks, but provides a lower uplink capacity. This is because switches in the ring stack can use only one uplink because the redundant uplink is blocked by STP for loop prevention.

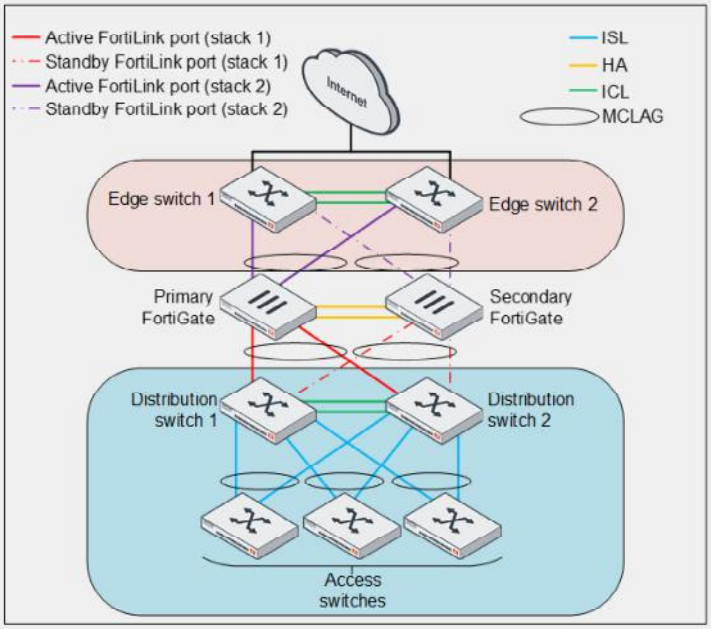
The topology shown on this slide implements redundancy in the LAN only. As shown in the next slide, you can deploy a second FortiSwitch stack on the internet edge, and use MCLAG to also achieve redundancy for your internet connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate Full Mesh HA with MCLAG

- Redundancy on both LAN and edge
- Two FortiSwitch stacks
  - LAN and edge
    - Each connected to different FortiLink interfaces
- Create second FortiLink interface on the CLI
  - GUI displays all FortiLink interfaces



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

You can deploy another pair of MCLAG peers on the internet edge to connect your FortiGate HA cluster to the internet. By using MCLAG to connect both the LAN and edge switches, you achieve a full mesh HA topology.

You must connect the new MCLAG peer group to a different FortiLink interface from the one used for the LAN switches. That is, you must configure a second FortiLink interface on FortiGate, and as a result, you will manage two different switch stacks. The latter is not a problem because FortiGate supports management of multiple switch stacks. However, you must create the second FortiLink interface on the FortiGate CLI. After that, the FortiGate GUI displays both FortiLink interfaces and switch stacks.

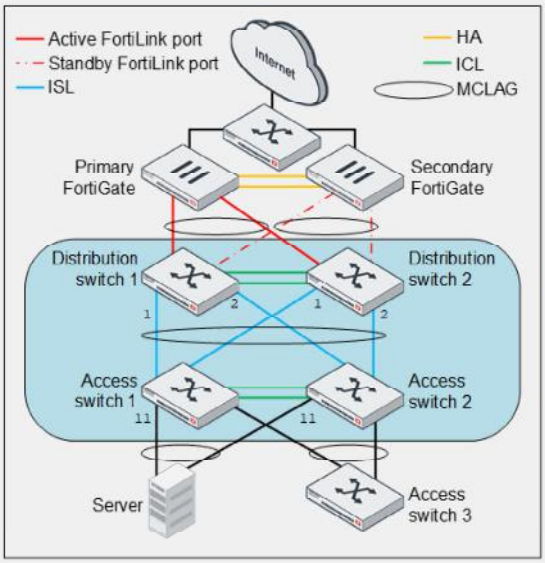
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate HA and Two-Tier MCLAG FortiSwitch Stack

- Configure a second MCLAG tier to connect
  - Critical devices that require MCLAG
- MCLAG configuration
  - Between MCLAG peer groups
    - Manual configuration required on upstream MCLAG peer group (distribution switch pair)

```
config switch auto-isl-port-group
    edit "access-pair-1"
            set members "port1" "port2"
    next
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

You can configure a second MCLAG tier on a pair of access switches to provide higher performance and redundancy to critical end devices, such as a server, or even another FortiSwitch.

Usually, MCLAG trunks automatically form after you connect FortiSwitch devices together and enable `mclag-icl` on the MCLAG peers. But, when you connect two pairs of MCLAG peer groups, on the upstream MCLAG peer group (the one closer to FortiGate), you must configure the ports that connect to the downstream MCLAG peer group. Based on the topology shown on this slide, if you want to use MCLAG trunks between the MCLAG peer group formed by the distribution switch pair and the MCLAG peer group formed by the access switch pair located just below, then, on the distribution switches, you must configure the ports that connect to access switch 1 and access switch 2. On the distribution switch pair, you must apply the configuration on the FortiSwitch CLI under the `config switch auto-isl-port-group` subsection.

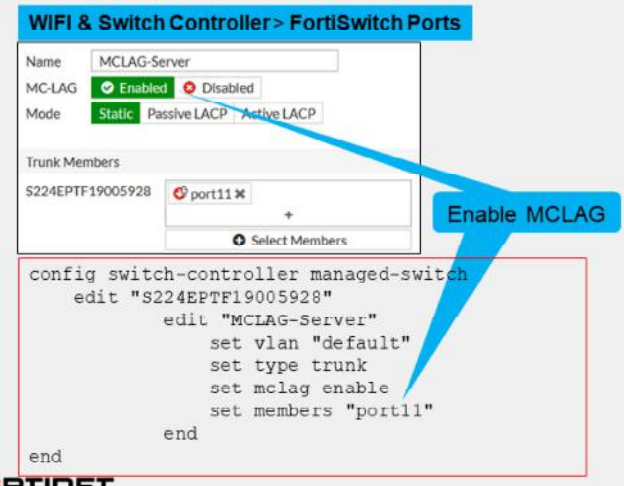
The topology on this slide indicates the ports that you must configure on the distribution switch pair. This slide also shows the FortiSwitchOS commands required for the configuration. Note that you must apply the auto-ISL port group configuration on both upstream MCLAG peers—each distribution switch in this case. In addition, the auto-ISL port group configuration on each switch must be *identical* for the MCLAG trunk between the two MCLAG peer groups to work.

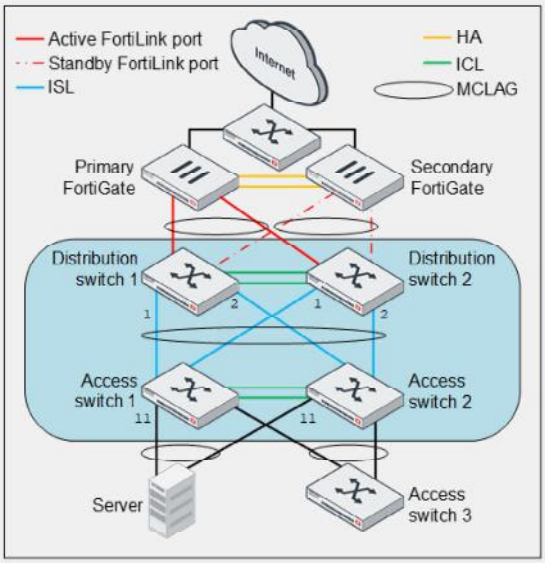
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate HA and Two-Tier MCLAG FortiSwitch Stack (Contd)

- MCLAG trunk configuration is:
  - Automatic for FortiLink trunks
  - Automatic for ISL on access switch 3
  - Manual for server:





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

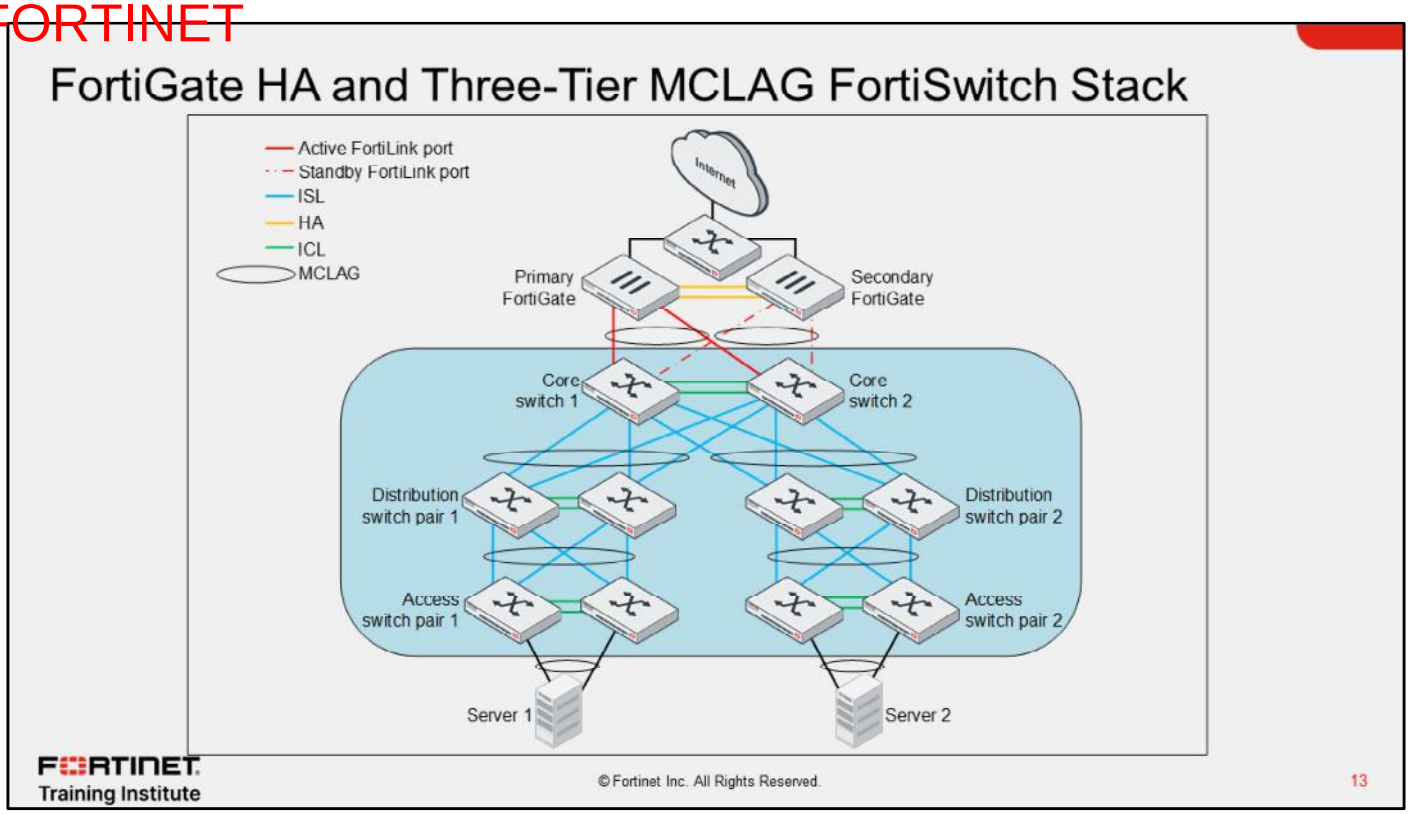
12

Except for enabling `mclag-icl` on the ICL ports that connect the distribution switch pair and the access switch pair, you don't need to apply any other configuration for the FortiLink trunks and the MCLAG trunk on access switch 3 to work, respectively. FortiSwitch creates these MCLAG trunks automatically for you.

However, you must manually configure the MCLAG trunk for the server on both access switch 1 and access switch 2. You do this on the **FortiSwitch Ports** page on the FortiGate GUI. Alternatively, you can run the FortiOS CLI commands shown on this slide. Note that you must apply the same configuration on both switches for the MCLAG trunk for the server to work.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

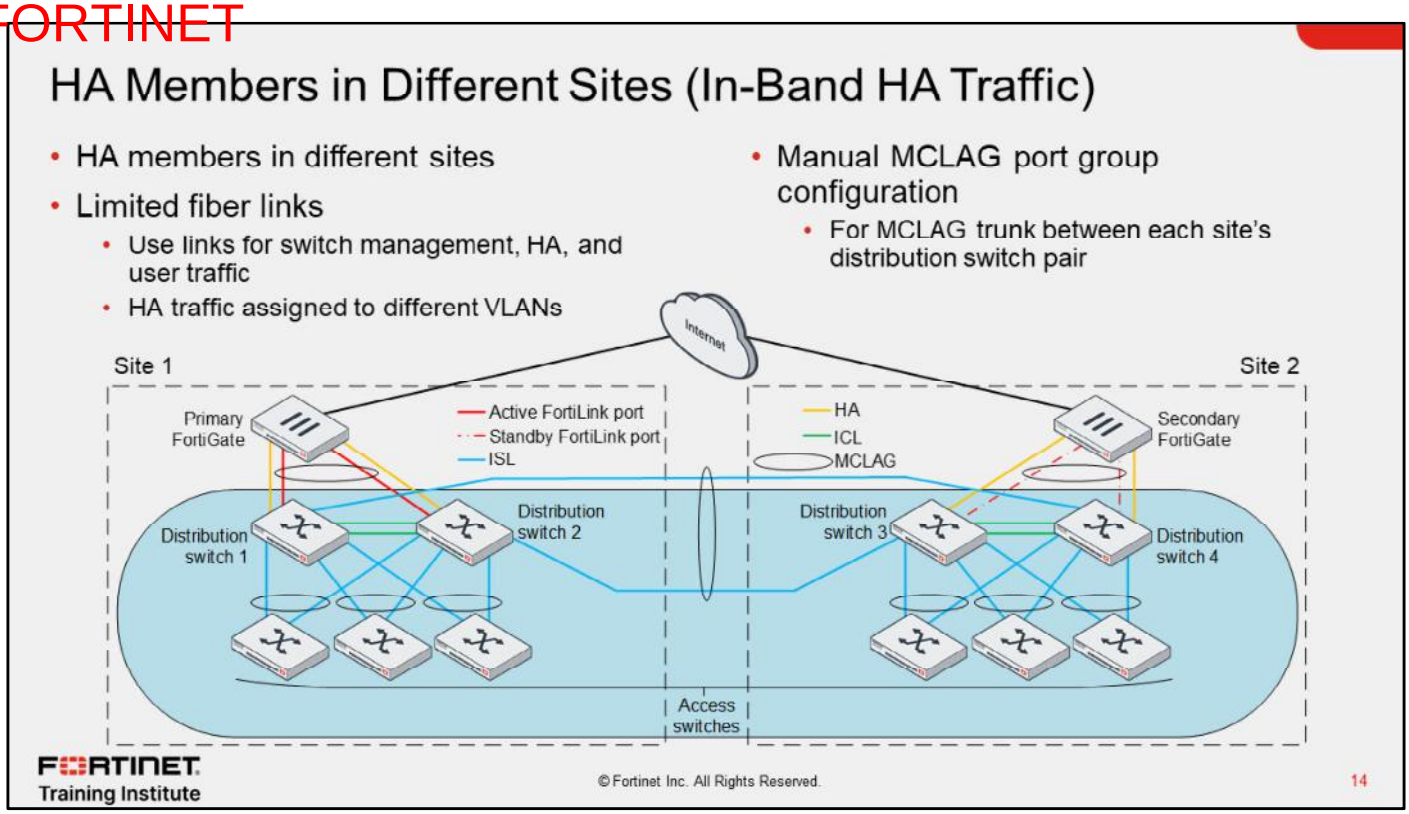


Usually, a one-tier or two-tier MCLAG deployment works for most networks. However, for some networks with a high number of distribution and access switches placed across different locations within a campus or large building, or in networks with large amounts of intra-VLAN traffic flowing within the distribution switch pairs, you may need to deploy another MCLAG peer group on top of the distribution switches that handles traffic destined only to FortiGate, such as inter-VLAN or internet traffic (north-south traffic), or traffic between different distribution switch pairs (east-west traffic). The additional MCLAG peer group, formed by the core switches in the topology shown on this slide, enables your network to scale more effectively when north-south and east-west traffic grow.

The topology on this slide shows three MCLAG tiers, one for each hierarchical layer: core, distribution, and access. Note that the core tasks are performed in conjunction with the core switches and the FortiGate HA cluster. In addition, like in the two-tier MCLAG deployment, you must configure the auto-ISL port groups for both the MCLAG trunks between the core switch pairs and the distribution switch pairs, and for the MCLAG trunks between the distribution switch pairs and the access switch pairs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can deploy a FortiGate HA cluster whose members are in different locations. For this setup, you usually use dedicated links to connect FortiGate HA ports. But what if you have a limited number of fiber connections between the sites? Is it possible to use the same fiber links to pass both switch management and user traffic while still being able to deploy HA and manage the switches on both sites?

In the example shown on this slide, there are two sites. On each site, there is a FortiGate device whose LAG members terminate on different FortiSwitch devices that are part of the same MCLAG peer group. For the HA setup, instead of connecting the FortiGate HA ports directly using dedicated fiber links, the HA ports are connected to the local distribution FortiSwitch pair. The goal is to use the two fiber links between the sites to transport both management and user traffic. To do this, on FortiGate, you create two different FortiSwitch VLANs that are used for HA traffic. Then, you assign these VLANs to the corresponding switch ports that connect the HA ports.

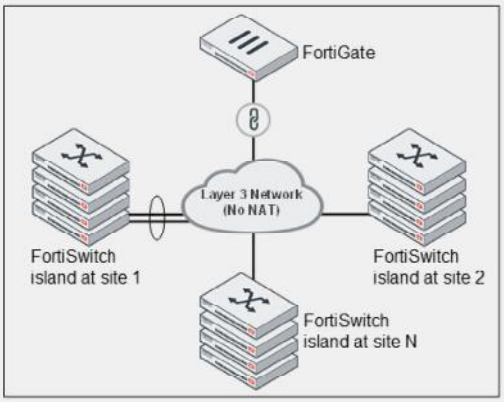
The switch ports that connect the distribution switch MCLAG pair on each site are used to carry switch management, HA heartbeat, and user traffic. In case the primary FortiGate fails, the secondary FortiGate takes over the HA cluster and the switch stack management. Like in the two-tier and three-tier MCLAG topologies, you must manually configure the auto-ISL port groups for the MCLAG trunk between the distribution switch pair on site 1 and the distribution pair on site 2 to work.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Management Over Layer 3

- Benefits
  - Cost-effective (one central FortiGate needed)
  - Less FortiGate devices to manage
- Requirements
  - No NAT in Layer 3 network
  - On FortiGate:
    - Configure FortiLink interface
  - On FortiSwitch:
    - Set target FortiLink interface IP or learn it through DHCP
    - Enable `fortilink-l3-mode` on ports facing FortiGate (if using internal interface)
- Limitations
  - No data path extension to switch controller
    - Switch configuration and monitoring only
    - Network devices in remote site must handle traffic



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

You can also manage FortiSwitch devices over a Layer 3 network that is fully routable. This is, no NAT is performed along the path. This is a cost-effective solution for large networks that have multiple groups of FortiSwitch devices—called islands—located on different sites, and that require being managed from a central FortiGate without having to deploy a FortiGate on each site. Not only do you reduce the FortiGate deployment costs, but you also avoid the administrative overhead of managing additional FortiGate devices.

When you manage FortiSwitch over Layer 3, FortiGate can discover FortiSwitch only after the switch starts the CAPWAP tunnel. That is, FortiGate doesn't use FortiLink or LLDP to discover the remote switches. Also, the user traffic in the islands is not sent to the switch controller, which means that the traffic must be handled by the network devices in the remote site. Also, the FortiSwitch VLANs you configure for a FortiSwitch island are used by FortiGate for configuration purposes only, and not for processing user traffic.

To manage a FortiSwitch island over Layer 3, you must:

- Configure the FortiLink interface on FortiGate
- Set the target FortiLink interface IP on FortiSwitch, or enable IP discovery through DHCP (option 138)
- Enable `fortilink-l3-mode` on the FortiSwitch ports facing the remote FortiGate, if you are using the internal interface for FortiGate communication

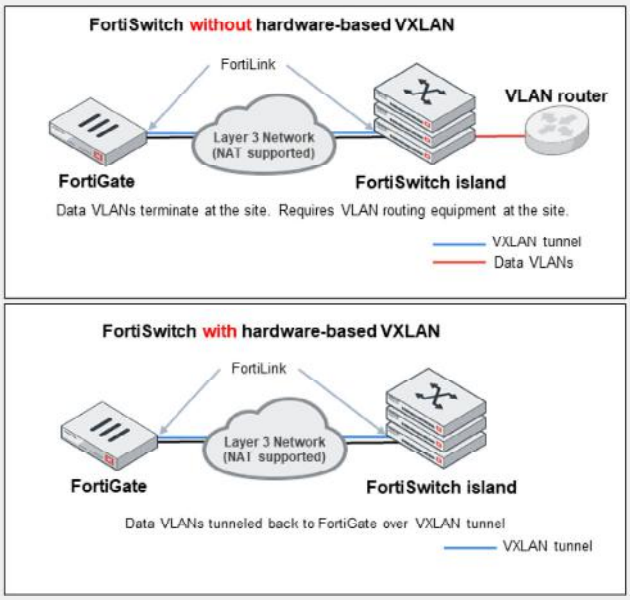
For FortiGate communication, you can use the management port or the internal interface on FortiSwitch. The former is an out-of-band option, and the latter is an in-band option. Using the internal interface enables you to use a LAG for management traffic, whereas using the management interface provides you with a dedicated physical port. You can use the internal interface for one FortiSwitch island and the management interface for another FortiSwitch island. However, you can't mix the interface types within a single FortiSwitch island.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Management Over Layer 3 (Contd)

- VXLAN
  - Virtual eXtensible LAN (VXLAN) can be used to create a Layer 2 overlay network over a Layer 3 network
  - Alternative method of tunneling FortiLink management connection over Layer 3 networks
- Benefits
  - Allows NAT in Layer 3 network due to frames being encapsulated in VXLAN protocol
  - Allows VLAN tunneling over Layer 3 networks for hardware-based VXLAN FortiSwitch devices
- Limitations
  - No data path extension to switch controller for FortiSwitch devices without hardware-based VXLAN
    - Switch configuration and monitoring only
    - Network devices at remote site must handle traffic



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

You can also manage FortiSwitch devices over a Layer 3 network by using a Virtual eXtensible LAN (VXLAN) tunnel to create a Layer 2 overlay network. VXLAN encapsulates Layer 2 frames into VXLAN protocol packets which can then be routed and have NAT applied, if required. Of the FortiSwitch devices that support VXLAN, a limited number are hardware-based VXLAN. Hardware-based FortiSwitch devices can also tunnel data VLANs in addition to switch management. Refer to the FortiSwitch Feature Matrix to determine which models support VXLAN FortiLink management and which support VLAN tunneling.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about the auto-ISL port group setting is true?
   A. You must always configure this setting when using MCLAG.
   ✓ B. You must configure this setting to form MCLAG trunks between different-tier MCLAG peer groups.

2. Which statement about the ring stack topology is true?
   A. It is not supported when connected to an MCLAG peer group.
   ✓ B. STP blocks the redundant uplink for loop prevention.

3. What is recommended for ICL trunks?
   ✓ A. Use at least two links for redundancy purposes.
   B. Never run STP on ICL trunks.

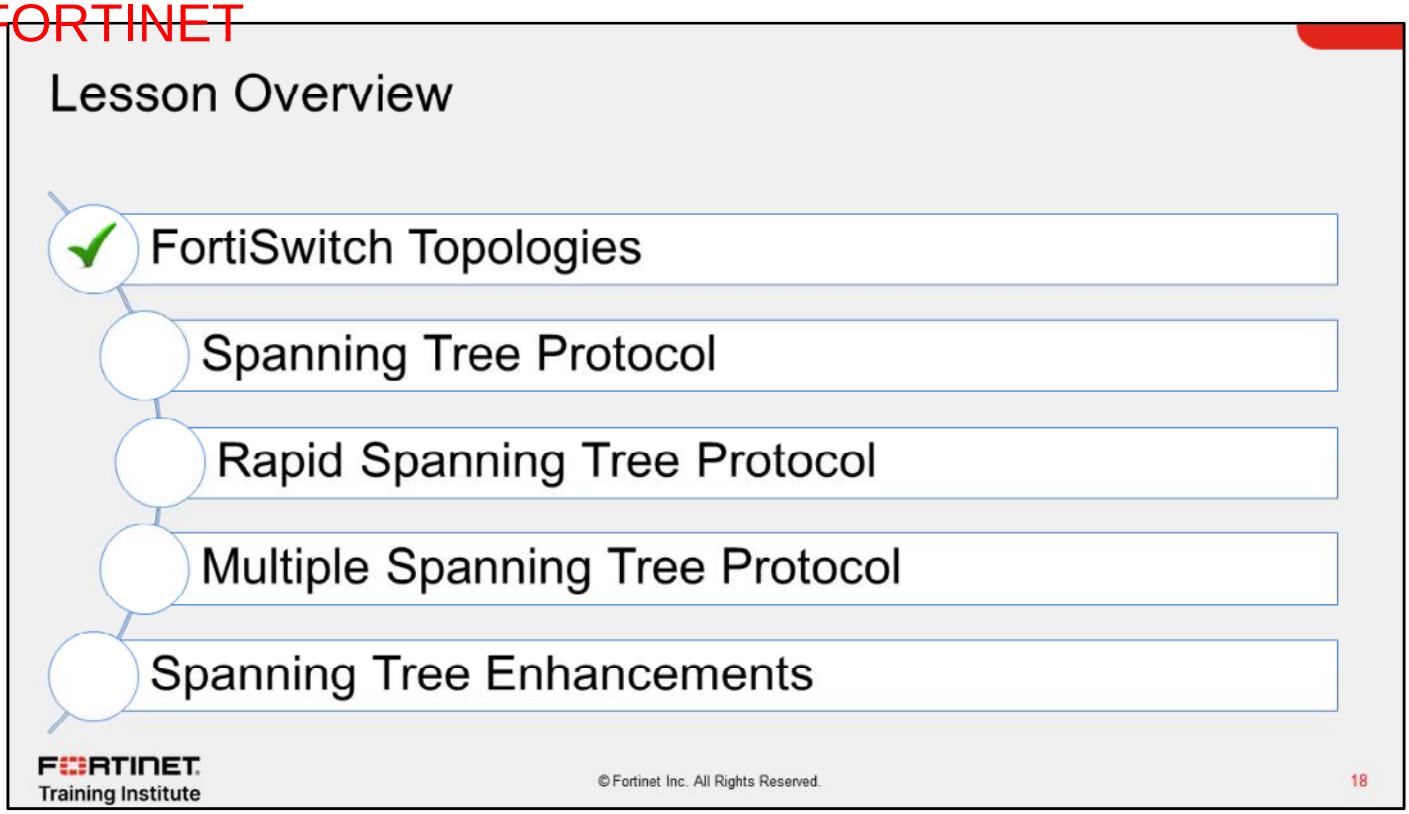
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

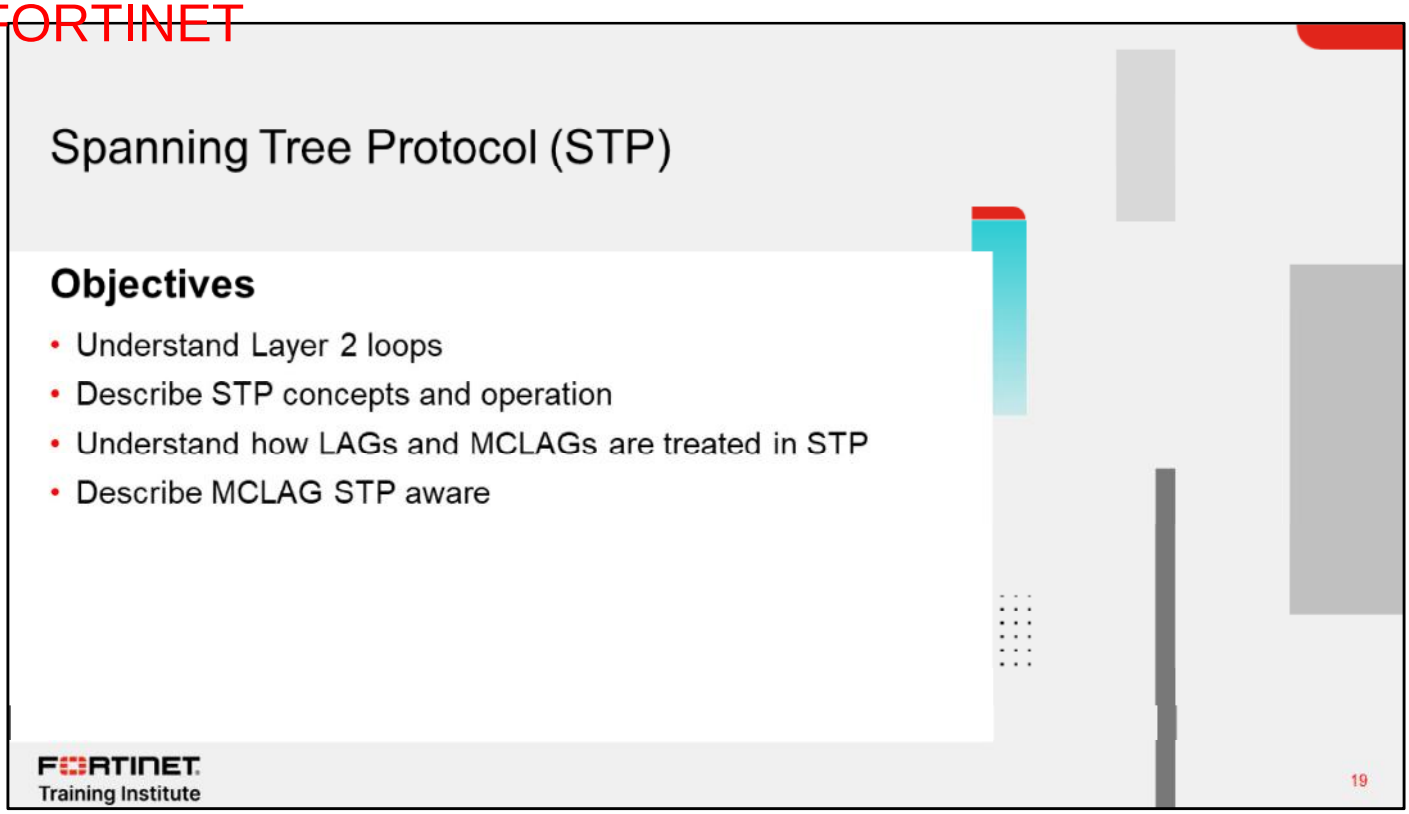


Good job! You now understand FortiSwitch topologies.

Now, you will learn about Spanning Tree Protocol (STP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

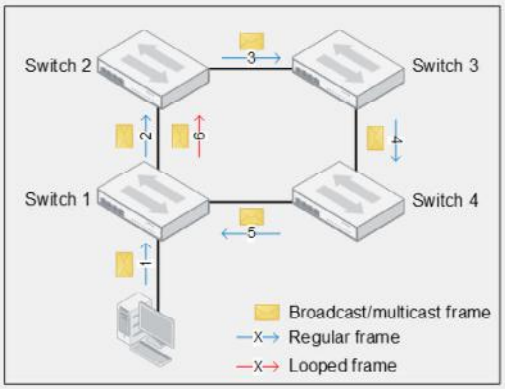
By demonstrating competence in STP, you will understand the fundamentals of loop prevention in Ethernet networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

The Layer 2 Loop Issue

- Use additional links for redundancy
  - Traffic continues flowing when a link fails
  - May cause Layer 2 loops
- Layer 2 loops impact performance due to:
  - Broadcast storms
    - Broadcast and multicast frames loop forever (no TTL)
    - Leads to insufficient network resources
  - MAC address table instability
    - Switches keep updating MAC address table entries
    - Leads to high CPU usage and starvation



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

To build resilient networks, network administrators often deploy additional links between switches to ensure that traffic continues to flow if one of the links fails. However, if no loop prevention method is in place, the multiple links may create a Layer 2 loop that results in broadcast storms and MAC address table instability.

Unlike IP packets, Ethernet frames do not have a time to live (TTL) attribute. This means that Ethernet frames disappear in the network only when they reach an endpoint or are dropped by a switch. A switch forwards broadcast and multicast frames to all its ports, except the port where the frame was received. If there is more than one active path between adjacent switches, the same broadcast and multicast frames that were initially forwarded by the switch are eventually received on the same switch, but on a different port. This results in the switch forwarding the same frames repeatedly. The traffic increases with every new broadcast and multicast frame sent by endpoints, which eventually leads to insufficient network resources to forward user traffic.

MAC address table instability is a result of broadcast storms, and occurs when a switch learns a MAC address on a port that is different from the port the MAC address was learned on previously. This is also known as MAC address flapping. The result is that the switch must update the MAC address table with the most recent port where the MAC address was learned. Because in a broadcast storm, the same broadcast and multicast frames are exchanged back and forth on different switch ports, the switches must update their MAC address tables after each exchange, which results in more CPU activity. The CPU usage becomes higher as the broadcast and multicast traffic grow. The increased CPU utilization may then slow down network traffic processing tasks performed by the switch, or even prevent them from running at all.

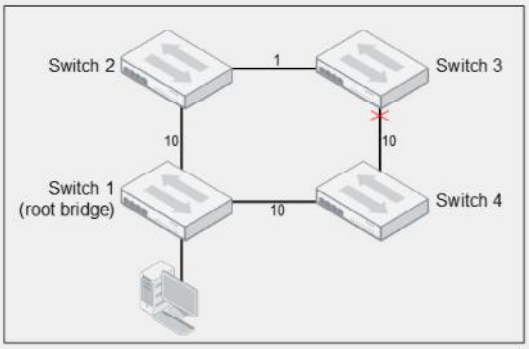
The example on this slide depicts a simplified Layer 2 loop. When the PC sends a broadcast or multicast frame to Switch 1, the switch forwards it to Switch 2, and this to Switch 3, and so on. When Switch 1 receives the frame from Switch 4, it forwards it again to Switch 2, starting the loop. Switch 1 must then update its MAC table because the MAC address of the PC has now been learned on the port that connects to Switch 4.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is STP (802.1D)?

- Builds Layer 2 loop-free logical topologies
- Switches
  - Exchange BPDUs to determine:
    - Root bridge (lowest bridge ID)
    - Cost of all links (higher bandwidth → lower cost)
    - Best root path (lowest accumulated cost)
  - Enable best link to root bridge and disable others
    - STP convergence is achieved after this
- STP reconvergence is triggered when:
  - New root bridge is detected
    - New root bridge election and best root path selection
- On root path failure:
  - New best link to root is selected
  - Alternate links to root are disabled



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

STP, which is defined in IEEE 802.1D, is a Layer 2 protocol that enables Ethernet networks to build loop-free logical topologies.

Switches that run STP, exchange Bridge Protocol Data Units (BPDUs) that contain information about the network topology. The switches then use the information in BPDUs to determine the root bridge and the cost of all links to the root bridge. The switch then enables the best link (cheapest) to the root bridge and disables all other more expensive links. The network achieves STP convergence after all switches determine the root bridge and the best link to it. Because STP disables the alternate links, the network becomes loop-free.

The switch with the lowest bridge ID is elected as the root bridge. The link with the lowest *accumulated* path cost to the root bridge is selected as the best link. The cost of a link is inversely proportional to its bandwidth. That is, the higher the bandwidth, the lower the cost, and vice versa.

A network STP reconvergence is triggered when switches detect a switch with a lower bridge ID than the current root bridge. This results in a new root bridge election and therefore, in the recalculation of the best link to the new root bridge.

When the best link to the root bridge fails, the switch ports for the alternate links go through a series of STP states to determine the new best link. Ultimately, the switch enables the new best link to the root bridge and disables all other links.

The example on this slide shows four interconnected switches running STP and the cost of each link. Switch 1 was elected as the root bridge. Therefore, the other three switches must build a loop-free topology towards the root bridge. The result is that STP disables the link between Switch 3 and Switch 4 to prevent a loop.

Vouchers & Dumps are Available | WhatsApp +201224560923

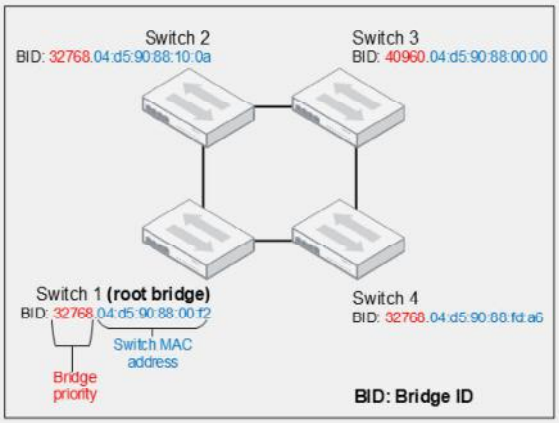
DO NOT REPRINT
© FORTINET
Brave-dumps.com

STP Root Bridge Election

- Bridge ID
  - Included in BPDUs sent by the switch
  - Concatenation of:
    - Bridge priority (default = 32768; configurable)
    - Switch MAC address (not configurable)

```
# get system status | grep Burn
Burn in MAC: 04:d5:90:88:fd:a6
```

- Election process
  - Initially, switches claim to be the root bridge
  - If a switch receives a BPDU with a lower bridge ID, it relays the new root bridge ID to neighbors
  - Election ends when all switches announce the same root bridge ID
- Lowest bridge ID calculation
  - Lowest bridge ID priority (first tiebreaker)
  - Switch MAC address (last tiebreaker)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

The first step for STP convergence is to determine the root bridge. The switch with the lowest bridge ID is elected as the root bridge.

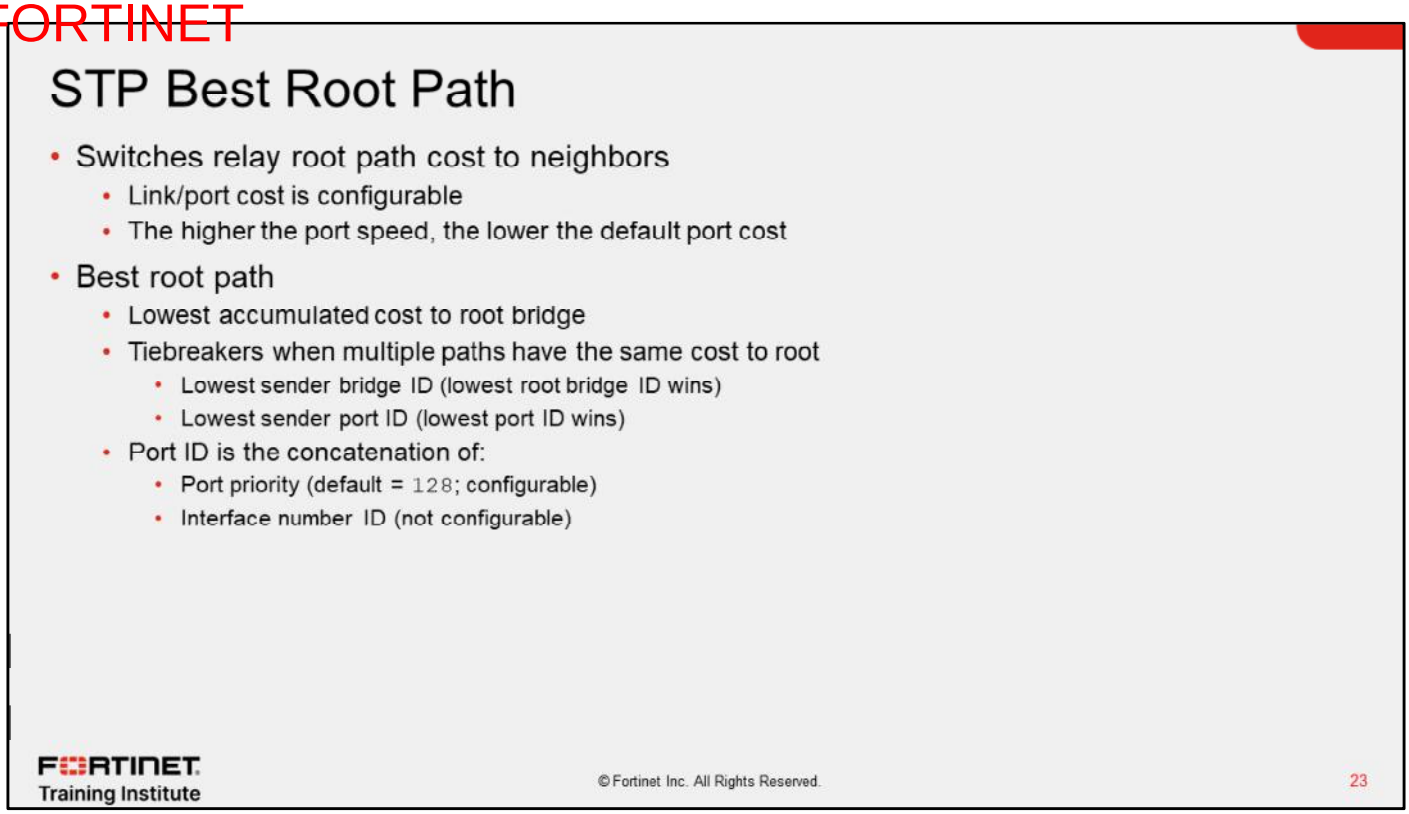
A switch includes its bridge ID in its BPDUs. When switches are powered on, they send BPDUs to the network and initially announce themselves as the root bridge. Later, if a switch receives a BPDU that contains a lower bridge ID, the switch stops advertising itself as the root bridge, and instead, relays the lower bridge ID to its neighbors. The process repeats itself on every switch in the network, and ends when all switches advertise the same root bridge ID.

The bridge ID is the concatenation of the bridge priority and the switch MAC address. You can configure the bridge priority, but not the switch MAC address. This means that you can influence the root bridge election by adjusting the bridge priority. On FortiSwitch, the default bridge priority is 32768. You can look up the switch MAC address by running the `get system status` command on the FortiSwitch CLI, and then looking at the `Burn in MAC` line in the output.

When comparing two bridge IDs, the switch first compares the bridge priority. If the bridge priority is the same, the switch uses the switch MAC address as the tiebreaker. That is, the bridge ID with the lowest MAC address wins. In the example shown in this slide, Switch 3 has the highest bridge priority number, which automatically discards it as the root bridge. The other three switches have the same bridge priority, so their MAC addresses are used as the tiebreaker. When comparing the MAC address of each switch, Switch 1 has the lowest MAC address, and for that reason, is elected as the root bridge in the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The second step for STP convergence is to determine the best path to the root bridge. The link with the lowest *accumulated* cost to the root bridge becomes the best root path.

A switch includes its root path cost in its BPDUs. The root path cost of a sender switch is the sum of the costs of each link that connects that switch to the root bridge. When an adjacent switch receives the BPDU, it adds the cost of the local link where the BPDU was received. The receiver switch then advertises its new root path cost to its neighbors.

When there is more than one link with the same cost to the root bridge, the switch uses the following tiebreakers to determine the best root path:

- Lowest sender bridge ID: Used when multiple upstream switches have the same root path cost. The lowest bridge ID wins.
- Lowest sender port ID: Used when multiple equal-cost upstream links that are *not* part of a LAG connect to the same switch. The lowest port ID wins.

The port ID is the concatenation of the port priority and the interface number. You can configure the port priority and cost, but not the interface number. This means that you can influence the best root path selection by adjusting the priority and cost on ports. On FortiSwitch, the default port priority is 128. The default port cost depends on the port speed. The higher the speed, the lower the cost, and vice versa.

Vouchers & Dumps are Available | WhatsApp +201224560923

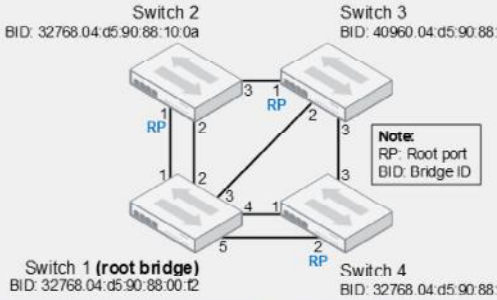
DO NOT REPRINT
© FORTINET
Brave-dumps.com

STP Best Root Path (Contd)

- Switch 1 is the root bridge (lowest bridge ID)
- Root port (RP): port connected to the best root path
- RP election on each switch
  - Switch 2
    - Sender port ID is the tiebreaker for port1 and port2
      - Port1 is RP because the sender port ID has a lower interface ID
  - Switch 3
    - Link through Switch 2 has a lower accumulated cost
      - Port1 is RP
  - Switch 4
    - Sender port ID is the tiebreaker for port1 and port2
      - Port2 is RP because the sender port ID has a lower priority

Port Attribute	Port		
	1	2	3
Cost	1	1	1
Priority	128	128	128

Port Attribute	Port		
	1	2	3
Cost	1	3	4
Priority	128	128	128



Port Attribute	Port				
	1	2	3	4	5
Cost	1	1	1	1	1
Priority	128	128	128	128	32

Port Attribute	Port		
	1	2	3
Cost	1	1	4
Priority	128	128	128

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

The example on this slide shows four interconnected switches, the ports in use, and the port costs and priorities configured on each switch. The port that connects to the best root path is called the root port. The root bridge is Switch 1 because it has the lowest bridge ID. As a result, the other switches must identify the port that connects to the best path to Switch 1, that is to say, their root port.

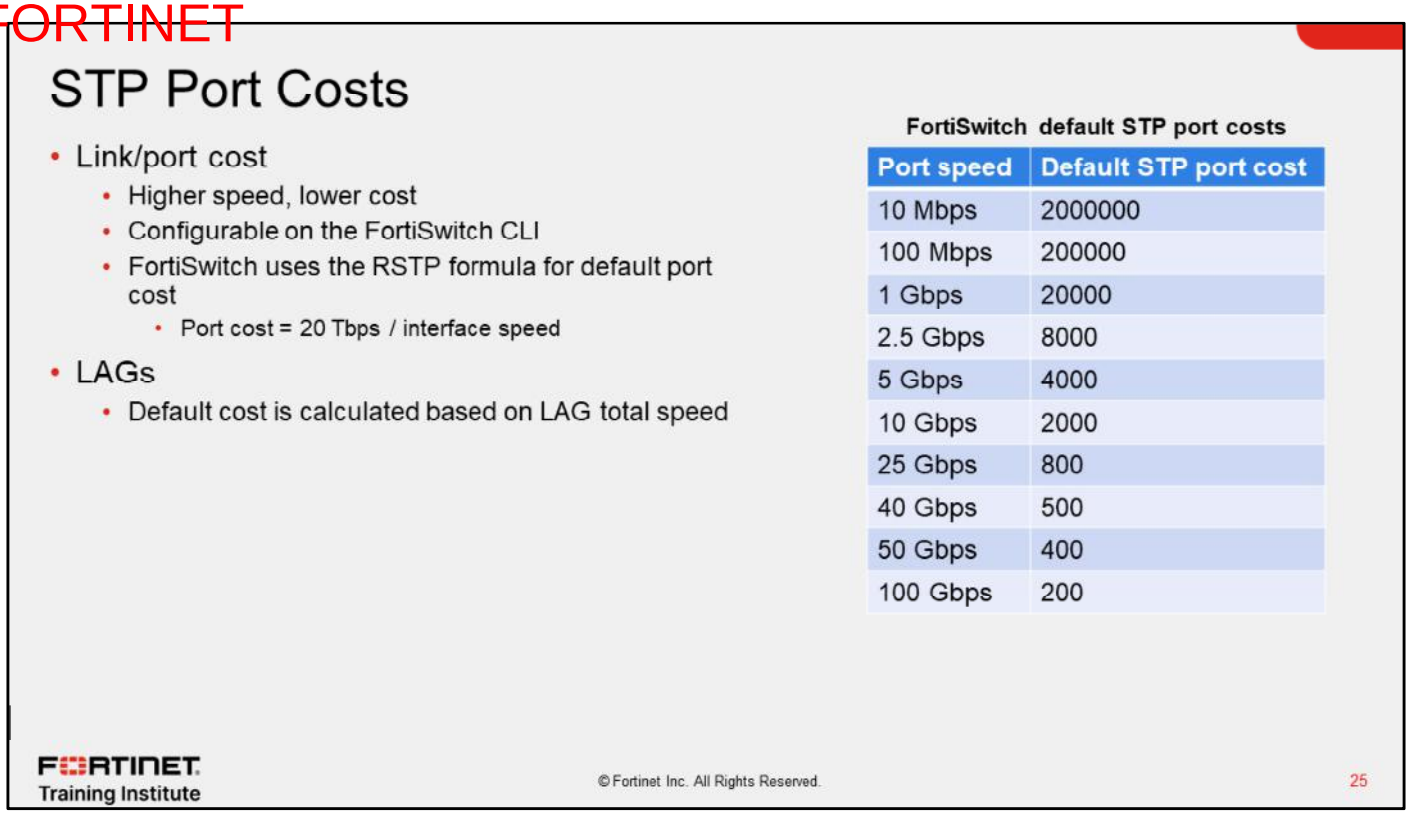
- Switch 2: The path with the lowest cost to the root bridge is through port1 and port2. Both ports are connected to the same switch (Switch 1), so STP uses the sender port ID as the tiebreaker. Both port IDs on Switch 1 have the same priority, so the port with the lowest interface ID wins, which is port1. Port1 on Switch 1 is connected to port1 on Switch 2, so port1 on Switch 2 becomes the root port.

- Switch 3: Even though the switch has a direct link to Switch 1, the path with the lowest *accumulated* cost to the root bridge is through port1. For this reason, port1 becomes the root port.

- Switch 4: It has two equal-cost links to the root. STP uses the sender port ID as the tiebreaker. Port2 becomes the root port because it is connected to port5 on Switch 1, which has the lowest port priority.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The cost of a link is the same as the cost of the port connecting that link. In this course, link cost and port cost are used interchangeably. The higher the port speed, the lower its cost.

You can configure the cost of a port on the FortiSwitch CLI. But in case you don't, FortiSwitch uses the formula defined in Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) to calculate the default cost of ports:

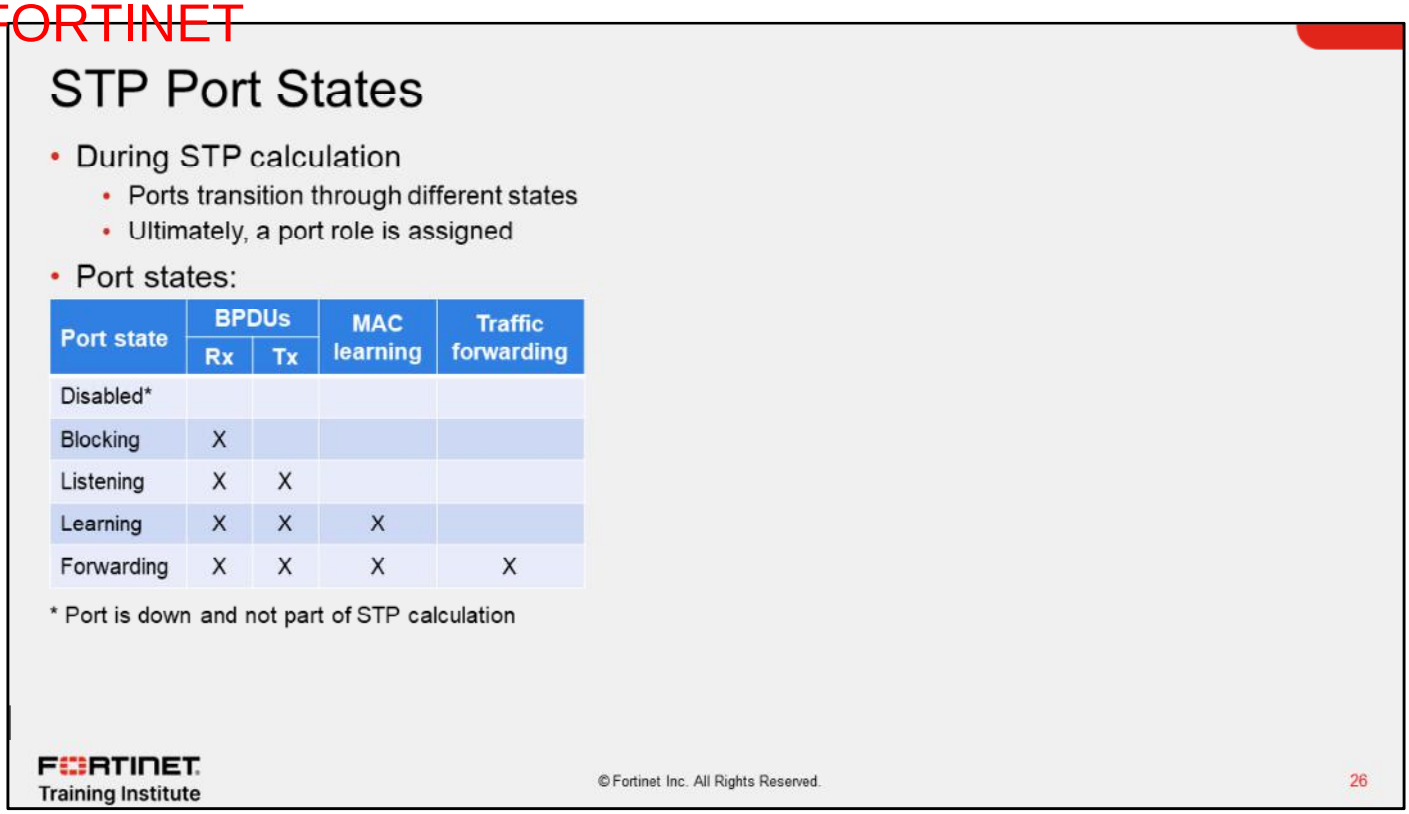
Port cost = 20 Tbps / interface speed

You will learn more about RSTP in this lesson.

The table on this slide shows the default port costs calculated by FortiSwitch based on the port speed. Note that the costs are for individual physical ports. When you bundle multiple ports together to form a LAG, a new logical interface with a higher bandwidth is created, and as a result, the new interface has a lower cost than its individual members. For example, if you form a LAG with two 100 Gbps ports, the default STP port cost for that LAG will be 100 because the LAG speed becomes 200 Gbps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you connect a switch or endpoint to the network, STP transitions the impacted ports through different states before the port is placed in the forwarding state. The following are the different STP port states:

- Disabled: The port is down and is not part of STP calculation.
- Blocking: The port receives BPDUs but does not send any. The port does not forward traffic either.
- Listening: The port receives and sends BPDUs but does not forward traffic.
- Learning: The port receives and sends BPDUs, populates its MAC address table, but does not forward traffic.
- Forwarding: The port is fully operational. It forwards traffic, receives and sends BPDUs, and populates its MAC address table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

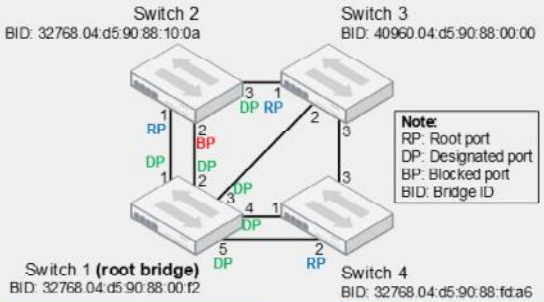
STP Port Roles

- Port roles:

Port roles	Traffic forwarding	Description
Root	X	- Best root path - One root port per switch
Designated	X	- All ports in root bridge are designated - The other end of a root port - Tiebreaker: non-root port with the best root path cost
Blocked		- Alternate path to root bridge - Blocking state for loop prevention - Switch can have multiple blocked ports - The other end of a blocked port is a designated port

Port Attribute	Port 1	Port 2	Port 3
Cost	1	1	1
Priority	128	128	128

Port Attribute	Port 1	Port 2
Cost	1	3
Priority	128	128



Port Attribute	Port 1	Port 2	Port 3	Port 4	Port 5
Cost	1	1	1	1	1
Priority	128	128	128	128	32

Port Attribute	Port 1	Port 2
Cost	1	1
Priority	128	128

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

During STP convergence, the port is assigned a role and placed in the forwarding or blocking state. The following are the different STP port roles:

- Root: The port that connects the switch to the best root path. A switch has only one root port.
- Designated: A non-root port that forwards traffic. All ports in the root bridge are designated ports. If one end of a link is a root port, the other end is a designated port. When the other end of the link is another designated port candidate, the port on the link with the best root path cost becomes the designated port and the other the blocked port.
- Blocked: A port that connects to an alternate path to the root bridge. The port is in the blocking state to prevent loops. A non-root bridge switch can have multiple blocked ports. On an alternate link, there is one blocked port only, which means that the other end of a blocked port must be in the forwarding state.

The example on this slide indicates the roles of all the ports in the topology. In this lesson, it is also explained how the root port on each switch is determined based on the STP best root path calculation. The roles of the non-root ports in the topology are determined as follows:

- Switch 1: The switch is the root bridge, so all its ports are designated ports.
- Switch 2:
  - Port2: The switch already has a root port (port1), so the port must be either a designated port or a blocked port. The port can't be a designated port because that would result in a loop. Therefore, the port is a blocked port.
  - Port3: The other end of the link is a root port, so the port is a designated port.

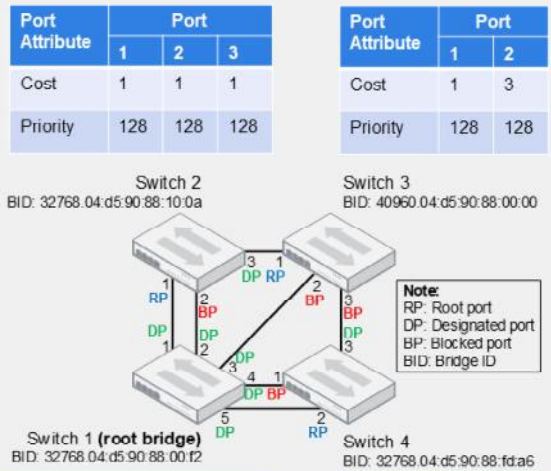
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

STP Port Roles (Contd)

- Port roles:

Port roles	Traffic forwarding	Description
Root	X	- Best root path - One root port per switch
Designated	X	- All ports in root bridge are designated - The other end of a root port - Tiebreaker: non-root port with the best root path cost
Blocked		- Alternate path to root bridge - Blocking state for loop prevention - Switch can have multiple blocked ports - The other end of a blocked port is a designated port



Port Attribute	Port 1	Port 2	Port 3
Cost	1	1	1
Priority	128	128	128

Port Attribute	Port 1	Port 2
Cost	1	3
Priority	128	128

Port Attribute	Port 1	Port 2	Port 3	Port 4	Port 5
Cost	1	1	1	1	1
Priority	128	128	128	128	32

Port Attribute	Port 1	Port 2
Cost	1	1
Priority	128	128

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

Now, let's determine the roles of the non-root ports on Switch 3 and Switch 4.

Port2 on Switch 3 and port1 on Switch 4 represent the same case as in port2 on Switch 2. That is, they must become blocked ports to avoid a loop in the network. However, for the ports connecting the link between Switch 3 and Switch 4, we need to identify which end of the link becomes the designated port and which one the blocked port. This is because the other end of a blocked port must be a designated port. For this reason, we need to use the following tiebreaker to identify the designated port on the segment:

- On a segment, the designated port is the non-root port with the best root path cost.

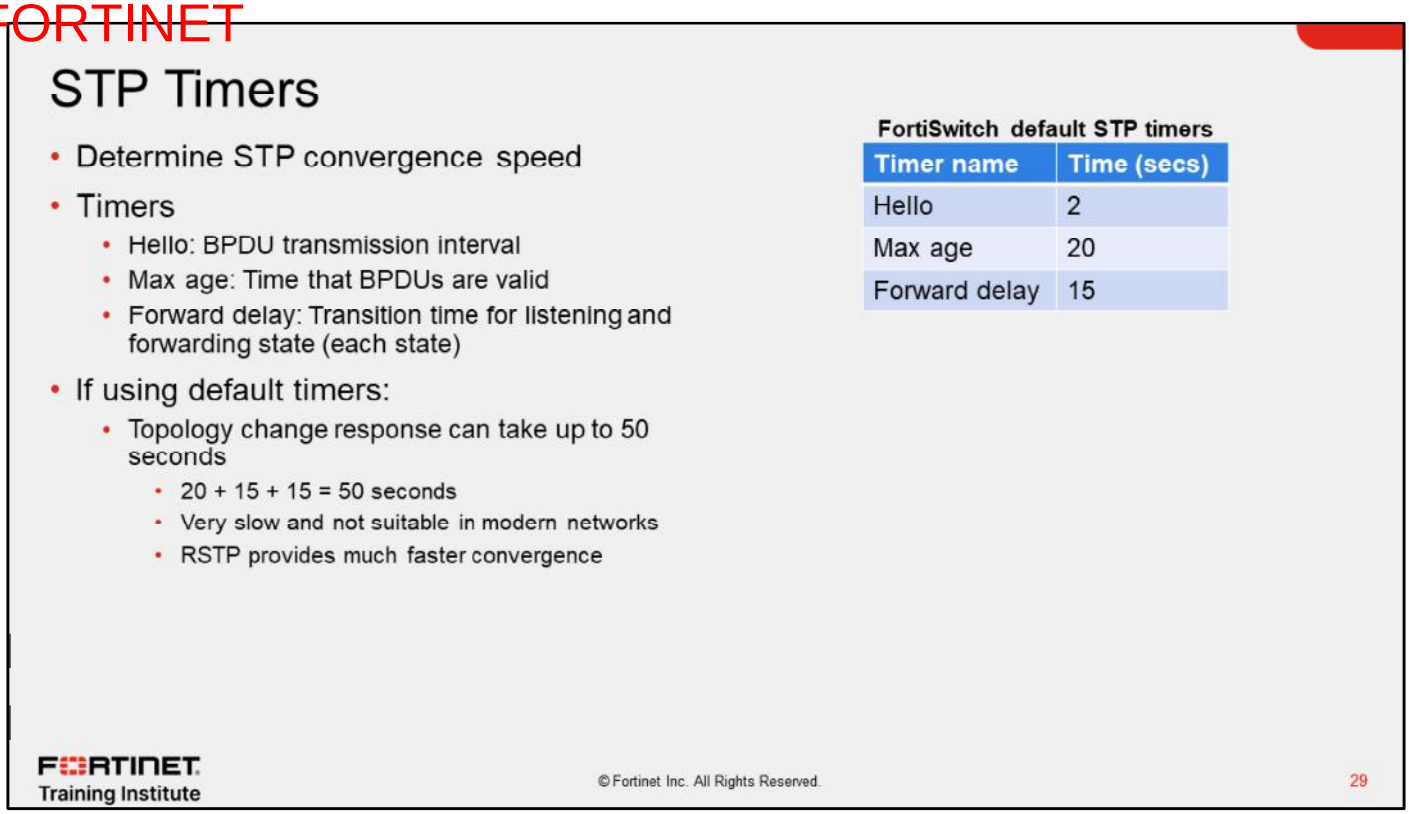
When comparing the root path cost from Switch 4 to Switch 1, which is 1, with the root path cost from Switch 3 to Switch 1, which is 2, the best root path is the one through Switch 4. For this reason, port3 on Switch 4 becomes the designated port and port3 on Switch 3 the blocked port.

If the root path cost for both switches is the same, the same additional tiebreakers used in the root bridge election are used for the designation port:

- Lowest sender bridge ID: Used when multiple upstream switches have the same root path cost. The lowest bridge ID wins.
- Lowest sender port ID. Used when multiple equal-cost upstream links that are *not* part of a LAG connect to the same switch. The lowest port ID wins.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The STP timers impact how fast STP responds to topology changes.

The root bridge sends BPDUs at the interval defined in the hello timer, which is two seconds by default. The non-root bridges then relay the BPDUs down the spanning tree network.

When a non-root bridge receives a BPDU, the configuration information contained in the BPDU is valid only for the time defined as the max age timer, which is 20 seconds by default. If a switch stops receiving BPDUs on a port for a period longer than the max age timer, the switch assumes that there has been a topology change, and moves the port to the listening state first, then to the learning state, and finally to the forwarding state. The time a port stays in the listening state and in the learning state before moving to the next state is defined by the forward delay timer, which is 15 seconds by default.

If a switch is using the default STP timer values, then STP may take up to 50 seconds to respond to a topology change, a waiting time that is considered extremely high in modern networks.

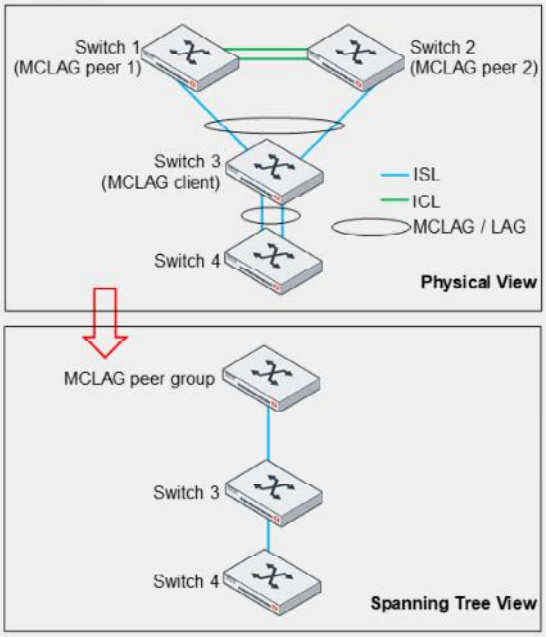
RSTP, which is defined in IEEE 802.1w, was designed to provide significantly faster convergence than STP, while still being backward compatible with STP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Spanning Tree in LAGs and MCLAGs

- LAGs and MCLAGs are often preferred for redundancy and higher performance
  - Simpler setup than MSTP
- Spanning tree sees:
  - LAGs and MCLAGs as single interfaces
    - No topology changes unless all LAG/MCLAG links come down
  - MCLAG peer group as a single switch



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

Network administrators often prefer to use LAGs and MCLAGs to enable redundancy and increase network bandwidth. Although you can achieve the same by using Multiple Spanning Tree Protocol (MSTP) and mapping VLANs to different instances, the setup is not as simple as when you use LAGs and MCLAGs. You will learn more about MSTP in this lesson.

From the spanning tree perspective, LAGs and MCLAGs are seen as a single logical interface. Also, LAGs and MCLAGs are considered up if at least one of their links is up. This means that changes in the state of the links in a LAG or MCLAG won't trigger a spanning tree topology change unless all the links in the LAG or MCLAG come down. In addition, in the case of an MCLAG peer group, the MCLAG clients see the two peers as a single switch participating in spanning tree.

The example on this slide shows four interconnected switches. Switch 1 and Switch 2 are MCLAG peers, and Switch 3 the MCLAG client. Switch 4 is connected to Switch 3 using a regular LAG. From the spanning tree point of view, the MCLAG peers are seen as a single switch, and the uplinks on Switch 3 and Switch 4 are treated as single interfaces.

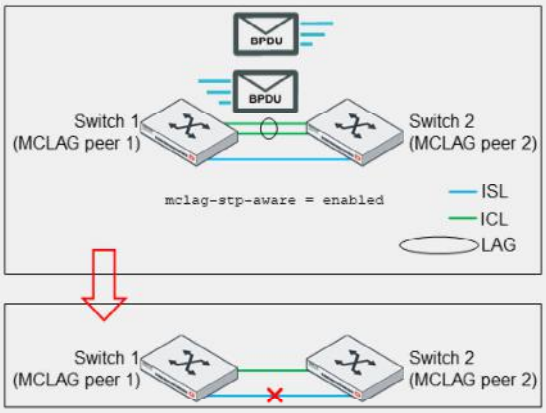
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

MCLAG STP Aware

- Enabled by default
- Enables spanning tree on ICL trunks
  - Ports on ICL trunks exchange BPDUs
    - BPDUs encapsulated in MCLAG control packets
  - Prevents loops by non-ICL links
- To enable or disable MCLAG STP aware on the FortiSwitch CLI:

```
config switch global
    set mclag-stp-aware enable | disable
end
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

The original MCLAG implementation did not run spanning tree on the MCLAG ICL trunks. Back then, if you added a non-ICL link between the MCLAG peers, you would have caused a loop in the network. The MCLAG STP aware feature, which is enabled by default, was then developed to address this issue.

When you enable MCLAG STP aware, MCLAG ICL trunks participate in STP. This means that the ports on the ICL links exchange BPDUs, which allows spanning tree to detect loops caused by non-ICL links between switches.

Note that the BPDUs are not exchanged by MCLAG peers in their original frame format. Instead, BPDUs are encapsulated in the MCLAG control packets that are exchanged by the MCLAG peers for MCLAG operation. In addition, the `mclag-stp-aware` setting is available on the FortiSwitch CLI only, and you can enable or disable it by running the commands shown on this slide.

This slide shows an example of a potential loop caused by a non-ICL trunk between two MCLAG peers. Because MCLAG STP aware is enabled, spanning tree can detect the loop and therefore, block the alternate path formed by the non-ICL link.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about Layer 2 loops is true?
   - ✓ A. Layer 2 loops cause broadcast storms and MAC address flapping.
   - B. Layer 2 loops do not impact CPU usage on a switch.

2. Which statement about STP operation is true?
   - A. The switch with the highest bridge ID is elected the root bridge.
   - ✓ B. You can influence root bridge election and best root path selection by adjusting STP settings.

3. How does STP treat LAG and MCLAG trunks?
   - A. LAG and MCLAG port members are treated as individual interfaces.
   - ✓ B. LAG and MCLAG trunks are treated as single logical interfaces.

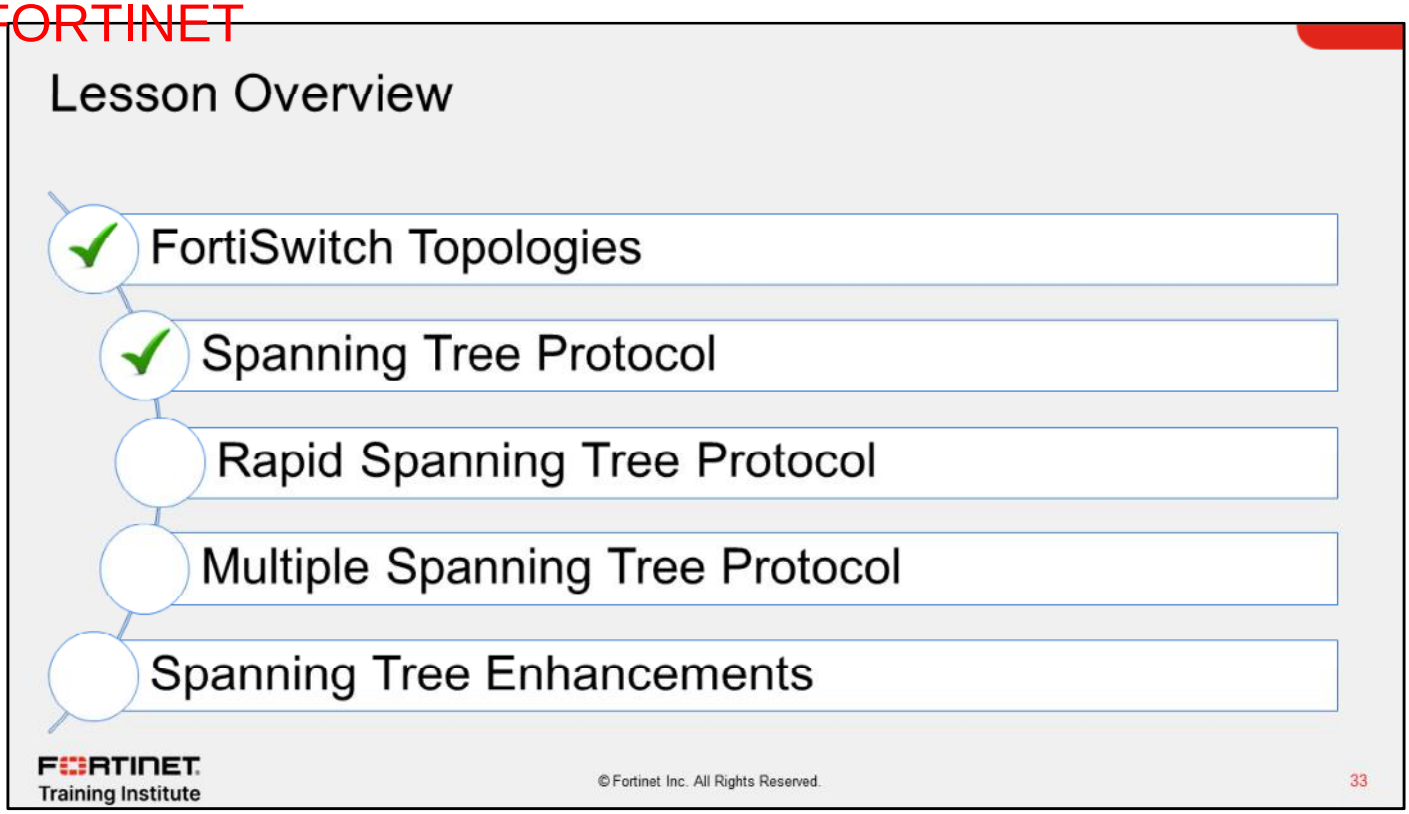
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

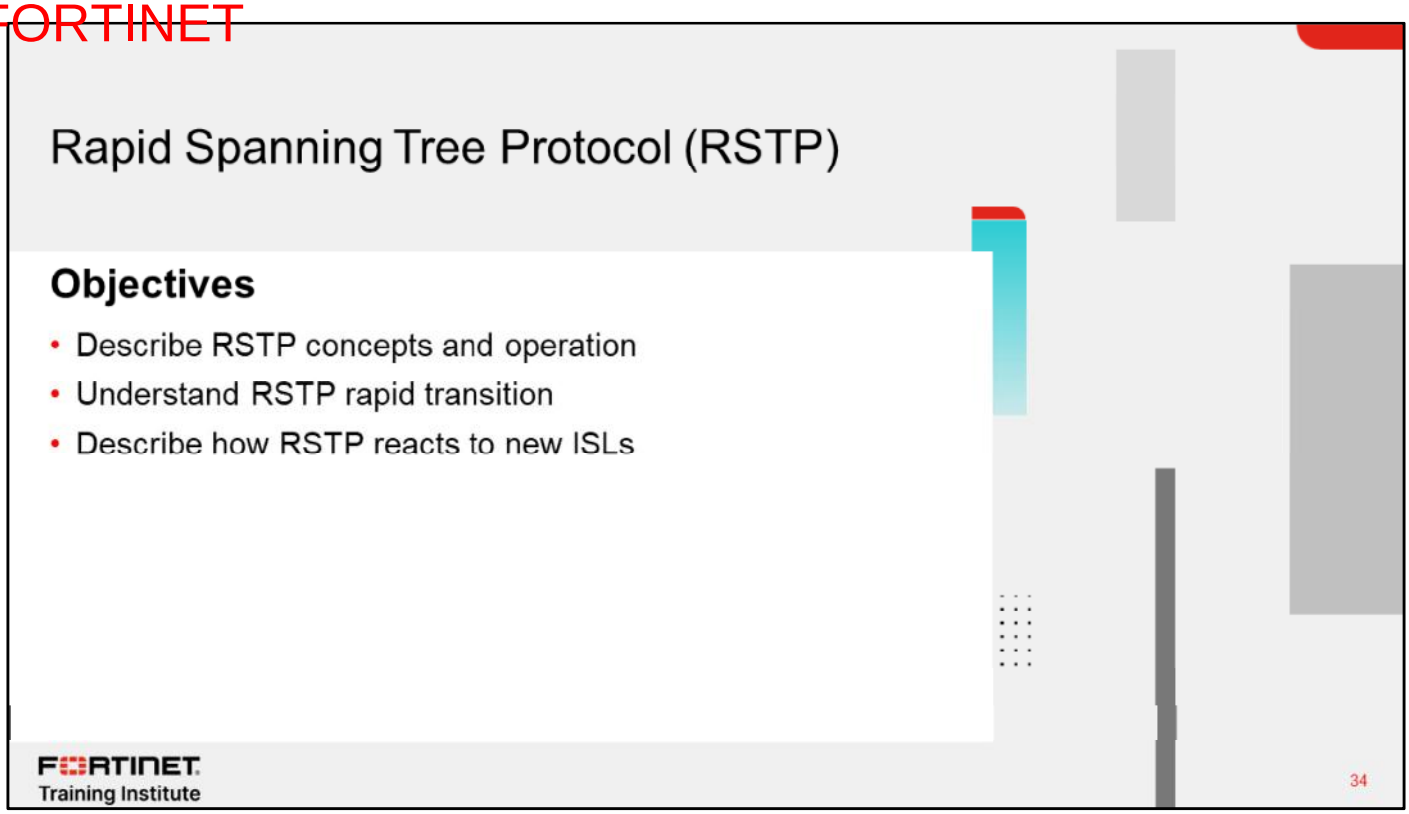


Good job! You now understand STP.

Now, you will learn about Rapid Spanning Tree Protocol (RTSP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

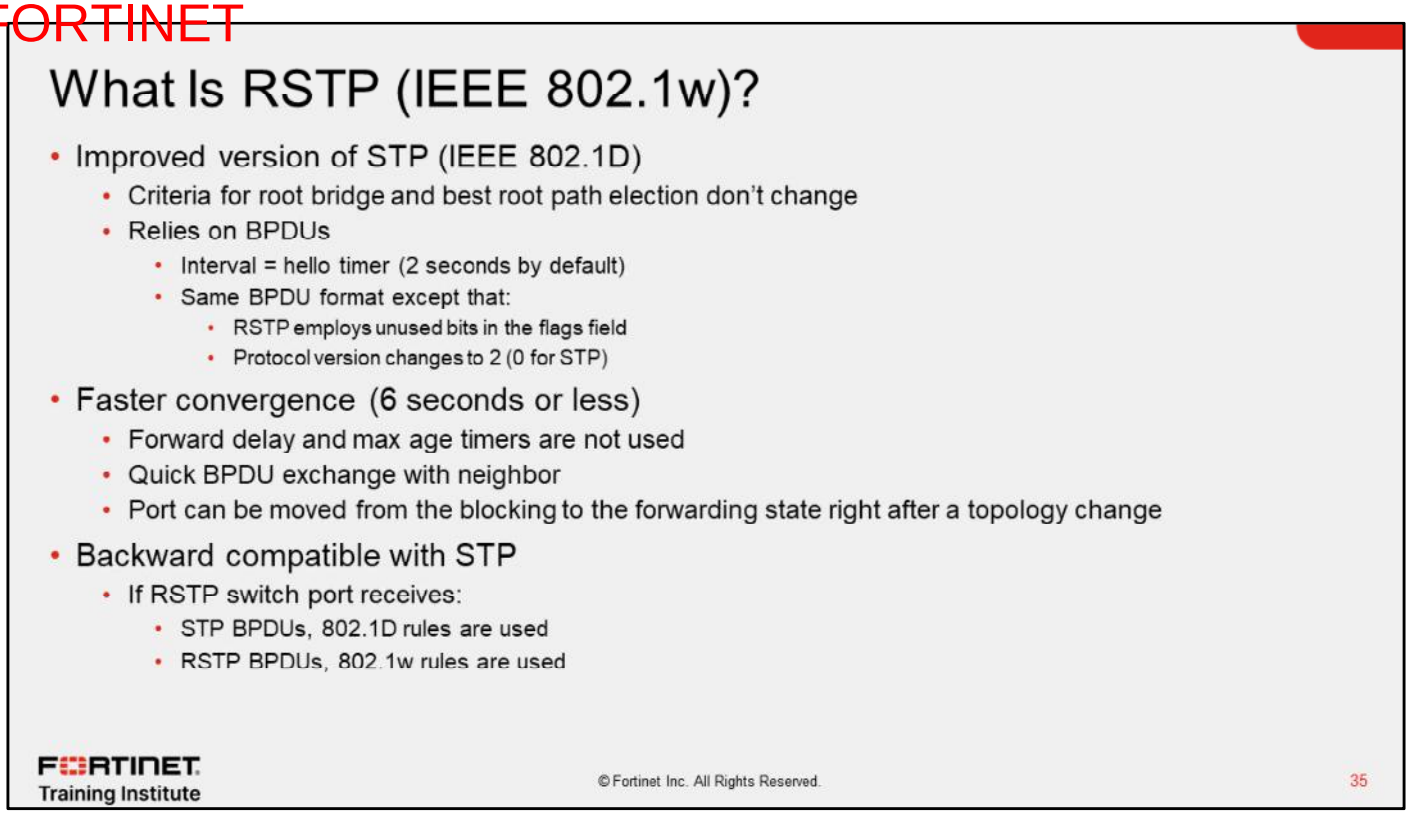


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in RSTP, you should be able to identify the enhancements made to STP to achieve faster network convergence.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



RSTP (IEEE 802.1w) is an improved version of STP (IEEE 802.1D) that addresses the long convergence times of its predecessor. RSTP uses the same STP criteria for root bridge election and best root path selection. Although RSTP introduces new port roles and states, the way the protocol determines the port roles and states is similar to STP.

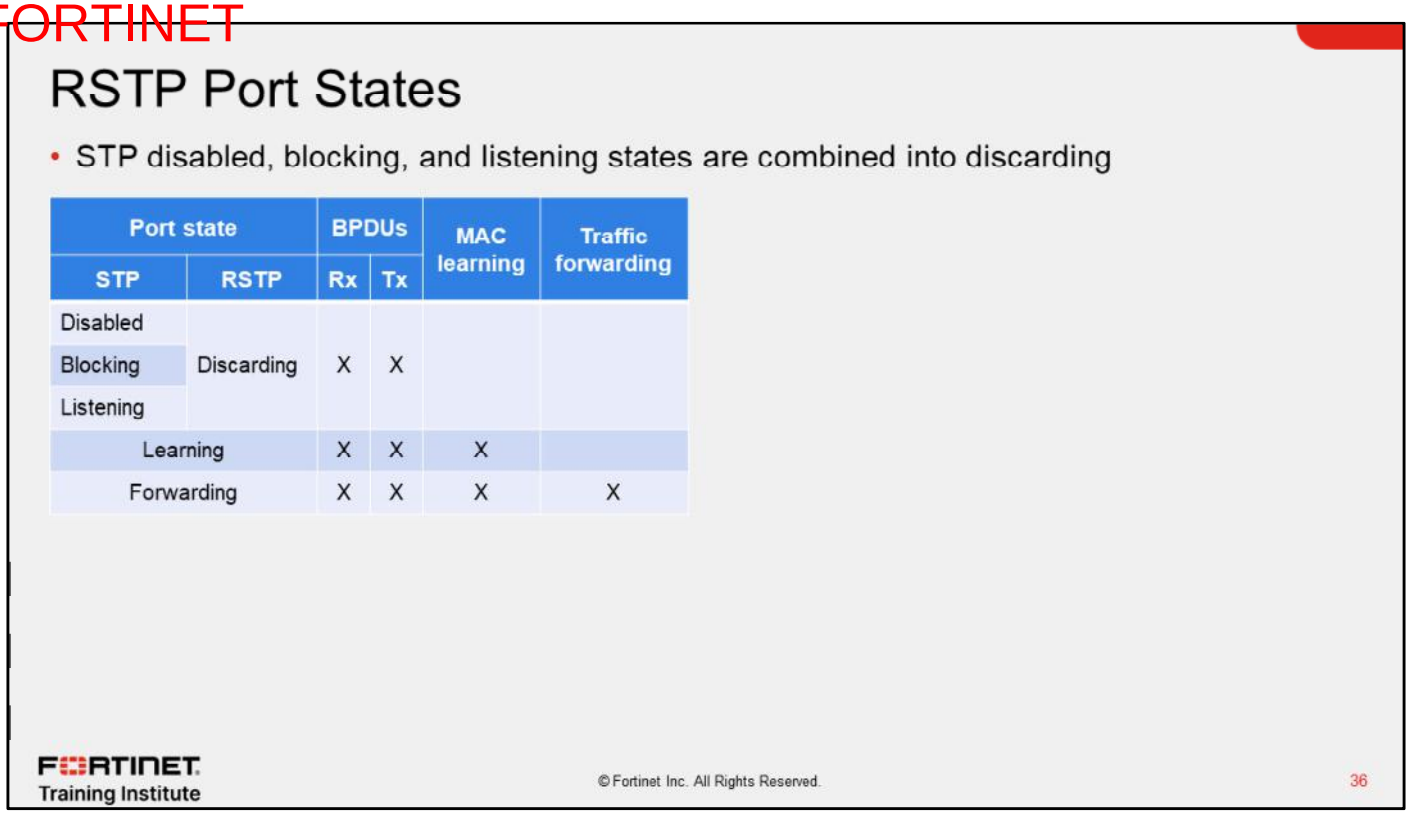
Like STP, RSTP relies on BPDUs to operate, which are sent at the interval defined by the hello timer (two seconds by default). The RSTP BPDU format is the same as in STP except that RSTP includes protocol-specific information in previously unused bits in the BPDU flags field. In addition, the protocol version in the BPDU is set to 2 to indicate RSTP, instead of 0 which is used for STP.

The most important benefit of RSTP is its much faster convergence to topology changes. With STP, the network takes between 30 to 50 seconds to converge, whereas in RSTP, it can take 6 seconds or less. RSTP provides faster convergence because it does not use the forward delay and max age timers used by STP when responding to network changes. Instead, the switch quickly exchanges BPDUs with the adjacent RSTP switch to determine the new port roles. In other cases, the switch just moves a blocking port to the forwarding state immediately after it detects the network change.

RSTP is backward compatible with STP. When an RSTP switch receives an STP BPDU on a port, the switch begins to use the 802.1D rules on that port. Conversely, if the switch receives RSTP BPDUs, the port operates according to the 802.1w rules.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



RSTP simplifies port states by combining the states that drop user traffic (disabled, blocking, and listening) into a new state called discarding. The other two states, learning and forwarding, behave the same as they do in STP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

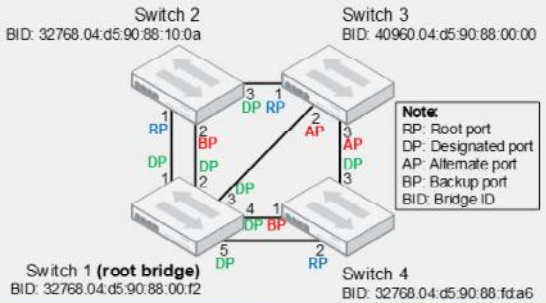
RSTP Port Roles

- STP blocking port split into two roles
  - Alternate
    - Less desirable path to root bridge
    - Different path from root port (different upstream switch)
  - Backup
    - Redundant (less desirable) port on a segment (same upstream switch)

Port role		Traffic forwarding
STP	RSTP	
Root		X
Designated		X
Blocked	Alternate Backup	

Port Attribute	Port		
	1	2	3
Cost	1	1	1
Priority	128	128	128

Port Attribute	Port	
	1	2
Cost	1	3
Priority	128	128



Port Attribute	Port				
	1	2	3	4	5
Cost	1	1	1	1	1
Priority	128	128	128	128	32

Port Attribute	Port	
	1	2
Cost	1	1
Priority	128	128

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

RSTP also introduces two new port roles that better define the role of the STP blocking port: alternate and backup. The other two port roles, root and designated, work the same as in STP.

An alternate port has a less desirable (higher cost) path to the root bridge than the root port, and is also connected to a different switch than the root port. A backup port is a redundant (less desirable) path to a segment where another (more desirable) port is already connected.

The example on this slide shows the port roles determined by RSTP for the same topology used in STP. The root ports and designated ports are determined by RSTP in the same way as by STP. However, for the backup ports, RSTP classifies them into alternate ports or backup ports. The roles of the alternate ports and the backup ports in the topology are determined as follows:

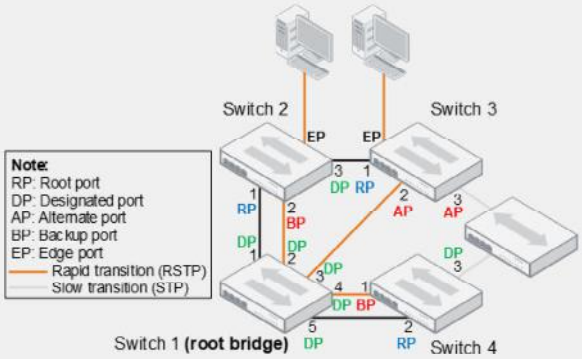
- Switch 2:
  - Port2: The port is connected to the same switch (same path to root) as port1. Therefore, port2 is a backup port.
- Switch 3:
  - Port2 and port3: The ports are connected to different switches from the one the root port is connected to (different paths to root). Therefore, both ports are alternate ports.
- Switch 4:
  - Port1: Like port2 on Switch 2, this is a backup port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RSTP Faster Transition to Forwarding

- Edge port (manual configuration)
  - A single endpoint connected to the port
    - No loops possible
  - Immediate transition to forwarding state after port comes up
- Alternate and backup ports (automatic)
  - Immediate transition to forwarding state after root port fails
    - Only on the port with the next best root path
- Link type (automatic)
  - Full-duplex ports considered point-to-point links
    - Rapid transition using RSTP negotiation and synchronization
  - Half-duplex ports considered shared ports
    - Legacy STP convergence is used (slow transition)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

When a port comes up or down in a network, STP must determine if there are changes in the port roles for the new topology. The ports which roles change from blocking to designated or root, go through the listening and learning states before being placed in the forwarding state. This means that the network does not converge before around 30 seconds have passed.

In contrast, RSTP provides much faster convergence because it does not rely on the STP timers to determine the port roles. Instead, it considers the following variables on a port:

- Edge port: This is a port that connects to a single endpoint. Because such a connection won't result in a loop, RSTP places edge ports in the forwarding state *immediately* after the port comes up. Edge ports send BPDUs and listen for incoming BPDUs. If an edge port ever receives BPDUs, the port loses its edge status and becomes a regular STP port. Note that you must manually configure the port as an edge port.

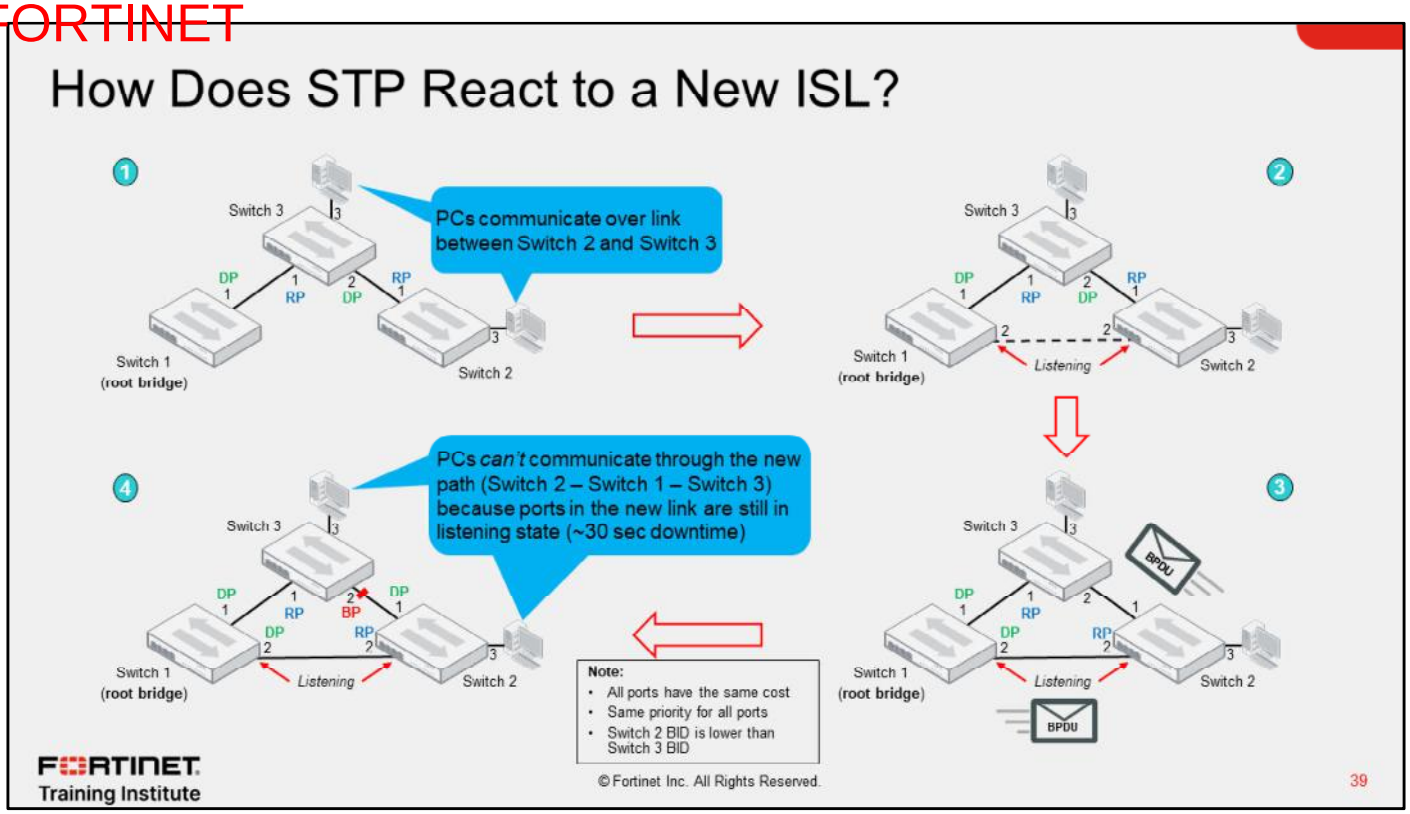
- Alternate and backup ports: Right after the root port on a switch fails, RSTP moves the alternate or backup port with the next best root path to the forwarding state, and then sets it as the new root port.

- Link type: Non-edge ports that operate at full-duplex are considered point-to-point links and therefore, candidates for fast transition to the forwarding state when the topology changes. For this, RSTP exchanges a proposal-agreement handshake to decide the state of each end of the link. Non-edge half-duplex ports, however, are considered connected to a shared medium, like a hub, where multiple switches may be also connected. RSTP then uses the traditional (and slower) STP convergence process on half-duplex ports.

In the example shown on this slide, the switch ports that connect to the PCs, are configured as edge ports. In addition, all switch ports, except those connected to the hub, operate at full-duplex. Consequently, on ports other than port3 on Switch 3 and port3 on Switch 4, RSTP can provide rapid transition to the forwarding state.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



RSTP provides faster convergence than STP when you add a link to a switch in your network. Before describing RSTP behavior, let's first explain how STP reacts to such a topology change and the time it takes for the protocol to converge.

1. The network is stable, and the roles of the ports have been determined from the root bridge (Switch 1) perspective. The PCs can communicate with each other through the link between Switch 2 and Switch 3.

2. A new link that connects port2 on Switch 1 and port2 on Switch 2 is added. The two ports will be placed in the *listening* state to check for incoming BPDUs. If the BPDUs are superior, the switches relay the BPDUs to their neighbors.

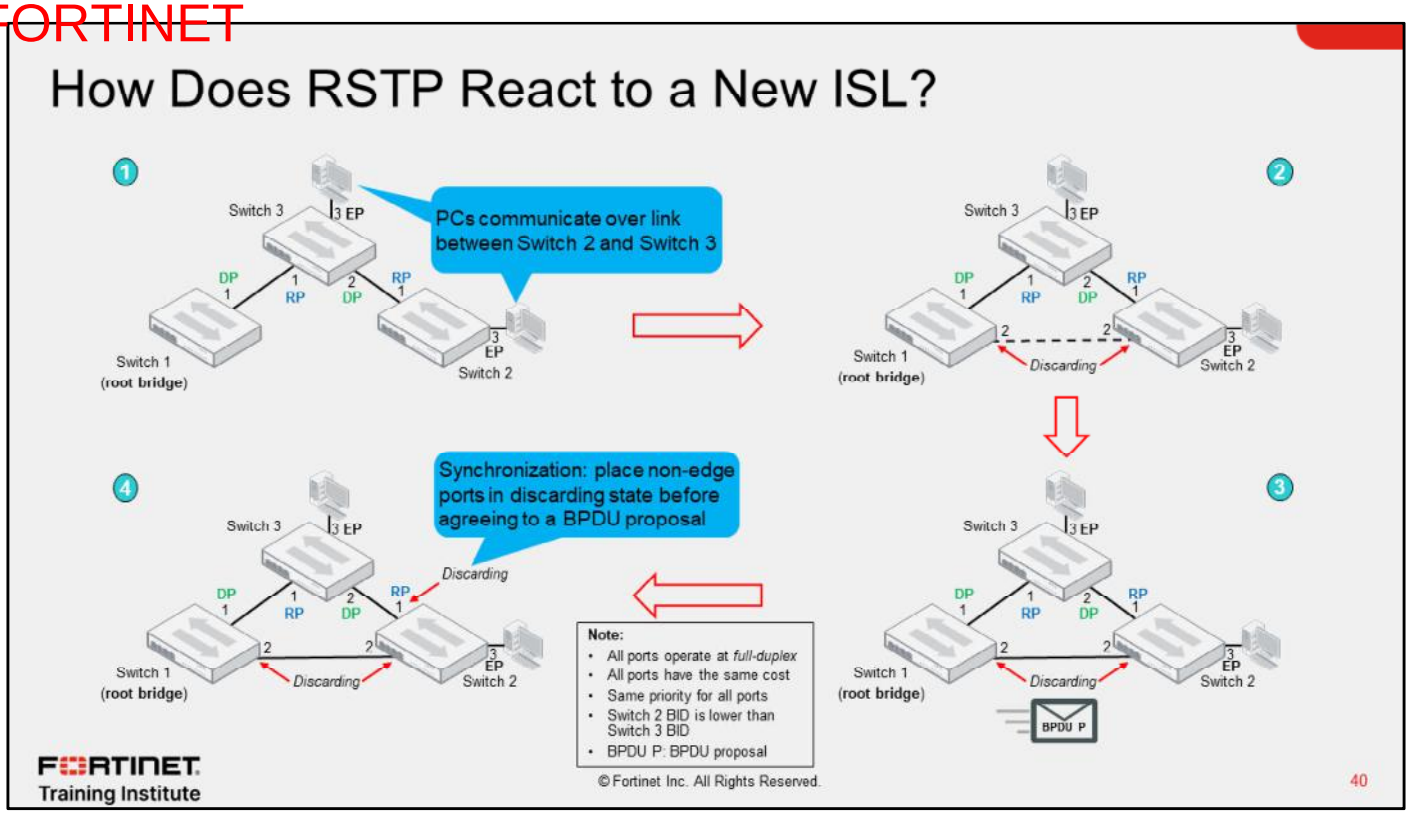
3. Switch 2 receives a superior BPDU (lower root path cost) on port2, and assigns the port as its new root port. Switch 2 also relays the superior BPDU to Switch 3. Switch 3 receives the BPDU from Switch 2, but does not consider it a better BPDU than the one received on port1, and therefore, does not relay it.

4. The link between Switch 2 and Switch 3 is now an alternate path to the root bridge and for this reason, is blocked by STP. Both switches have the same root path cost, but Switch 2 has a lower bridge ID, and therefore, port1 on Switch 2 becomes the designated port, and port2 on Switch 3 the blocked port.

The previous steps take place very quickly. That is, STP determines a new root path for Switch 2, and blocks the alternate path very quickly. However, port2 on Switch 1 and port2 Switch 2 still need to complete the transition through the listening and learning states before they start to forward traffic. This means that the PCs won't be able to communicate using the new path (through Switch 1) for the next 30 seconds or so, a waiting time that is considered unacceptable by today's availability standards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will learn about how RSTP reacts to the same topology change.

1. The network is stable, and the roles of the ports have been determined from the root bridge (Switch 1) perspective. The PCs can communicate with each other through the link between Switch 2 and Switch 3.

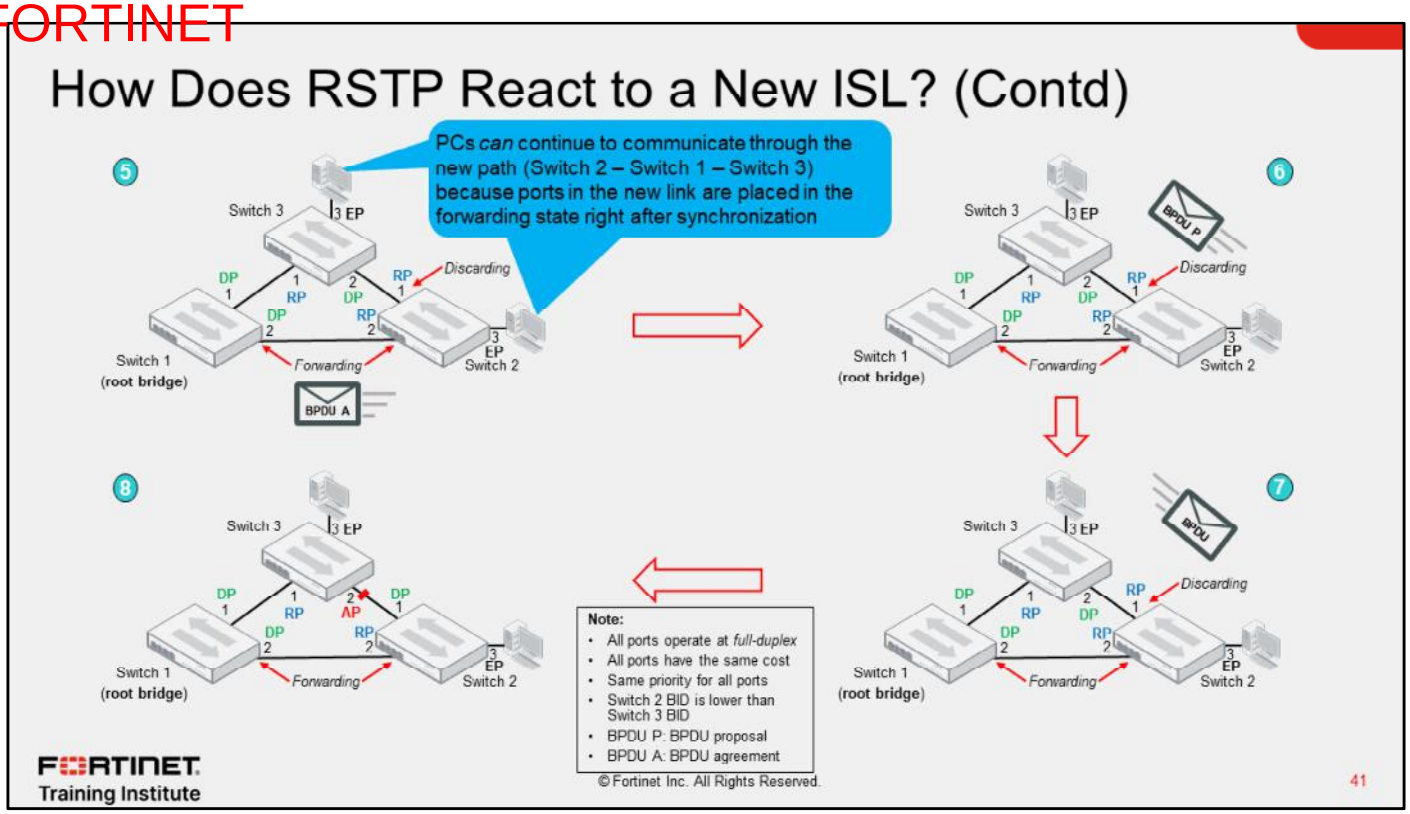
2. A new link that connects port2 on Switch 1 and port2 on Switch 2 is added. The two ports are placed in the *discarding* state to check for incoming BPDUs.

3. Switch 1 sends a BPDU *proposal* to Switch 2 to let Switch 2 know that it has a superior BPDU (Switch 1 is the root bridge).

4. Switch 2 realizes that Switch 1 has a superior BPDU and therefore, that it must assign port2 as its new root port. But before doing that, Switch 2 places all its non-edge ports to the discarding state to ensure no loops are formed later, when the ports on the new link are moved to the forwarding state. The only non-edge port in Switch 2 is port1, and it's placed in the discarding state. This mechanism of placing non-edge ports in the discarding state, before the switch agrees to a superior BPDU proposal, is called *synchronization*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



5. Switch 2 sends a BPDU *agreement* to Switch 1 to indicate that it accepts the superior BPDU. Both switches then place their respective ports in the forwarding state, and assign their roles. Note that there is no loop in the network because port1 on Switch 2 is in the discarding state. From this moment on, the PCs can reach each other using the new path formed by Switch 2, Switch 1, and Switch 3.

6. Switch 2 sends a BPDU proposal on each non-edge port that is currently in the discarding state, which in this case, is only port1.

7. Switch 3 ignores the BPDU proposal from Switch 2 because it is receiving superior BPDUs from Switch 1 on port1. Instead of sending a BPDU agreement to Switch 2, Switch 3 sends its own superior BPDU to Switch 2.

8. Switch 2 and Switch 3 realize that the link between them is an alternate path to the root bridge, and therefore, must be blocked to prevent a loop. Both switches have the same root path cost, but Switch 2 has a lower bridge ID, and therefore, port1 on Switch 2 becomes the designated port, and port2 on Switch 3 the alternate port.

Like in STP, the previous steps also occur very quickly, and the resulting loop-free topology is also the same. However, unlike STP, RSTP does not use timers for transitioning the ports to the forwarding state. Instead, when the topology changes, RSTP uses a proposal-agreement handshake and synchronization mechanism between adjacent switches to quicky determine port states and roles, while also ensuring that the network stays loop-free. This process repeats itself on links connecting non-edge ports that were put into the discarding state during synchronization, and ends when adjacent switches ignore the sender's BPDU proposal, and RSTP blocks the alternate path.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about RSTP operation is true?
   - A. RSTP is not backward compatible with STP.
   - ✓ B. RSTP does not use timers to respond to topology changes.

2. Which statement about an alternate port is true?
   - A. It connects to the same upstream switch where the root port is connected.
   - ✓ B. It connects to a different upstream switch where the root port is connected.

3. What does synchronization mean in RSTP?
   - ✓ A. A switch places non-edge ports in the discarding state before agreeing to a BPDU proposal.
   - B. Switches synchronize the entries in their MAC address tables.

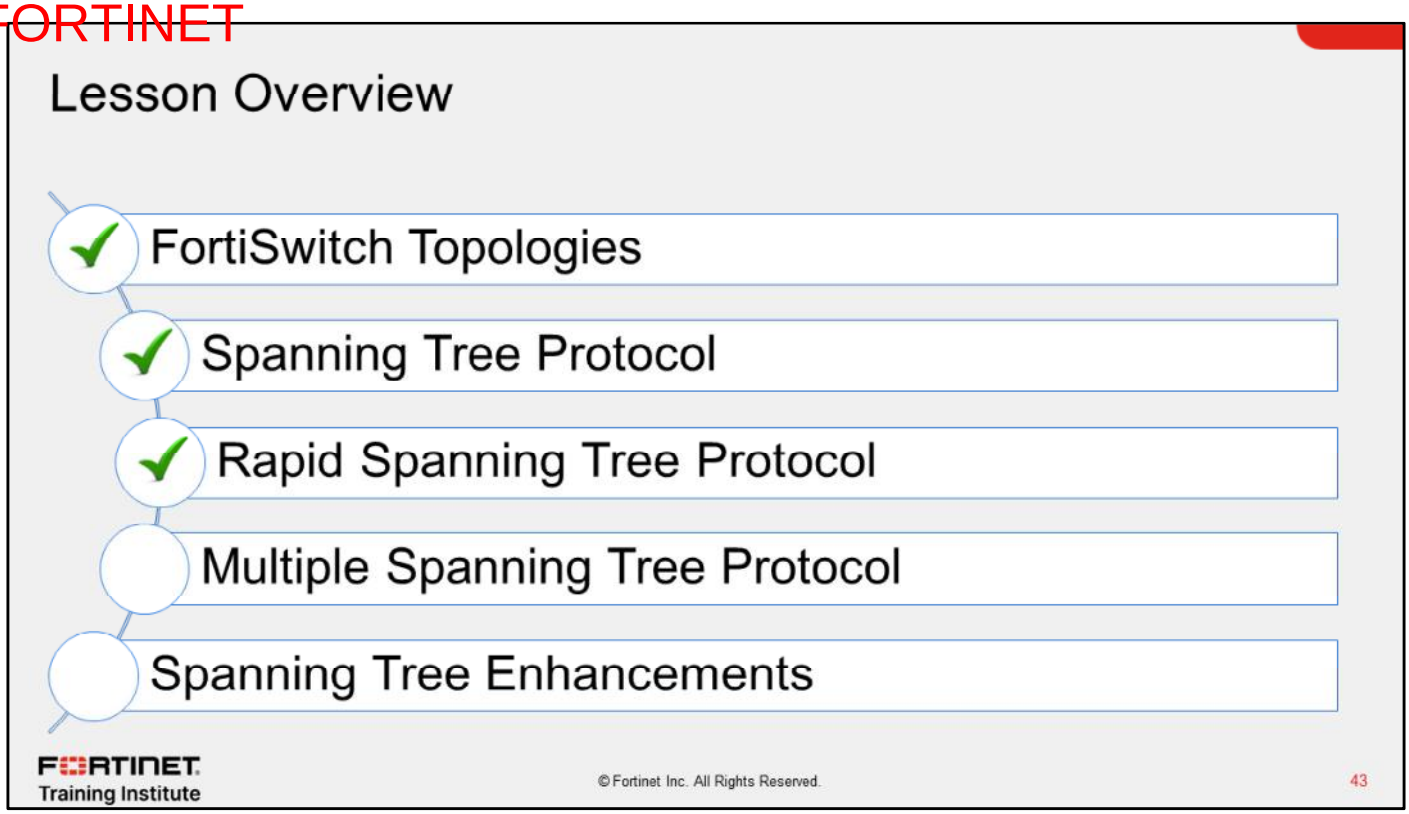
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

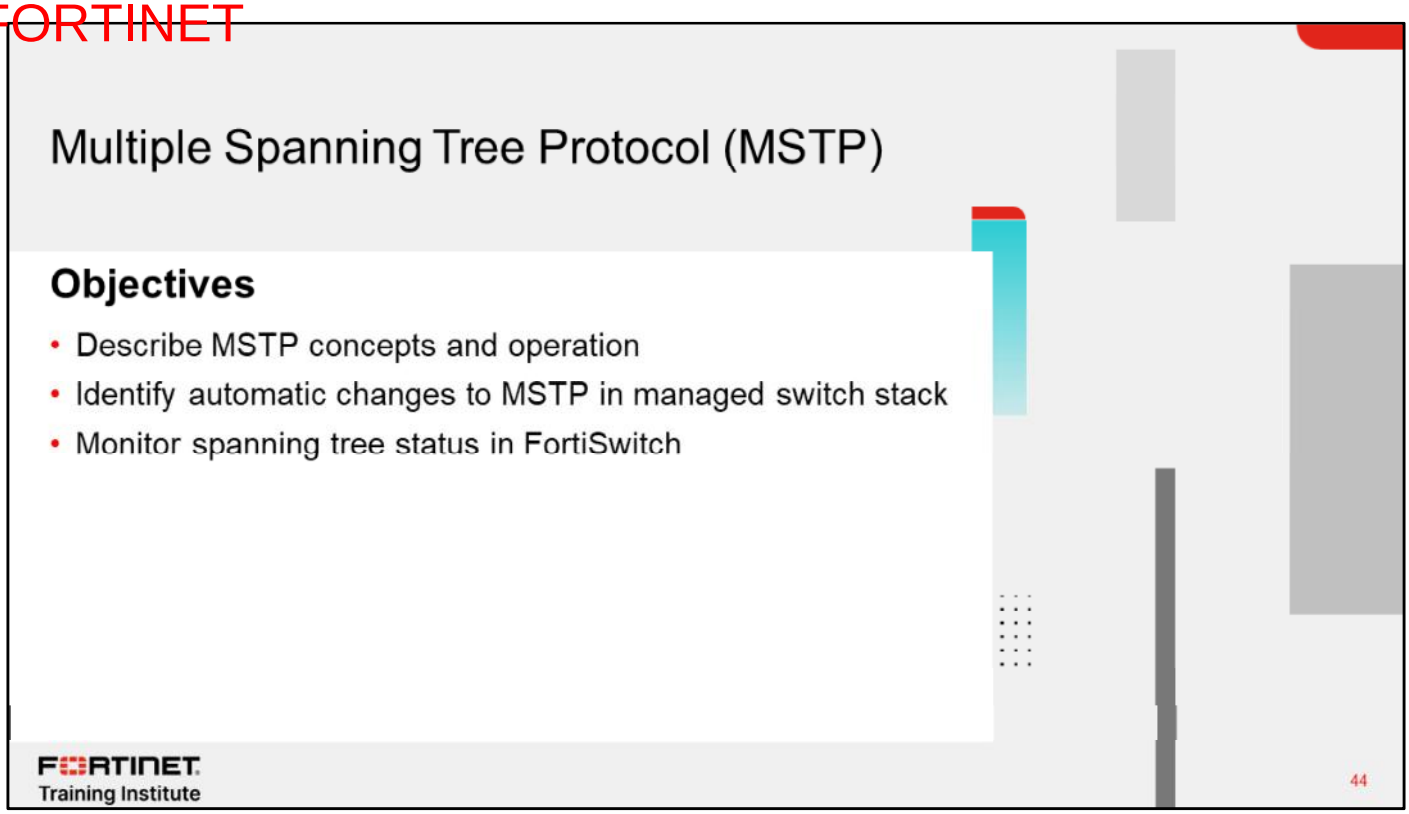


Good job! You now understand RSTP.

Now, you will learn about Multiple Spanning Tree Protocol (MSTP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

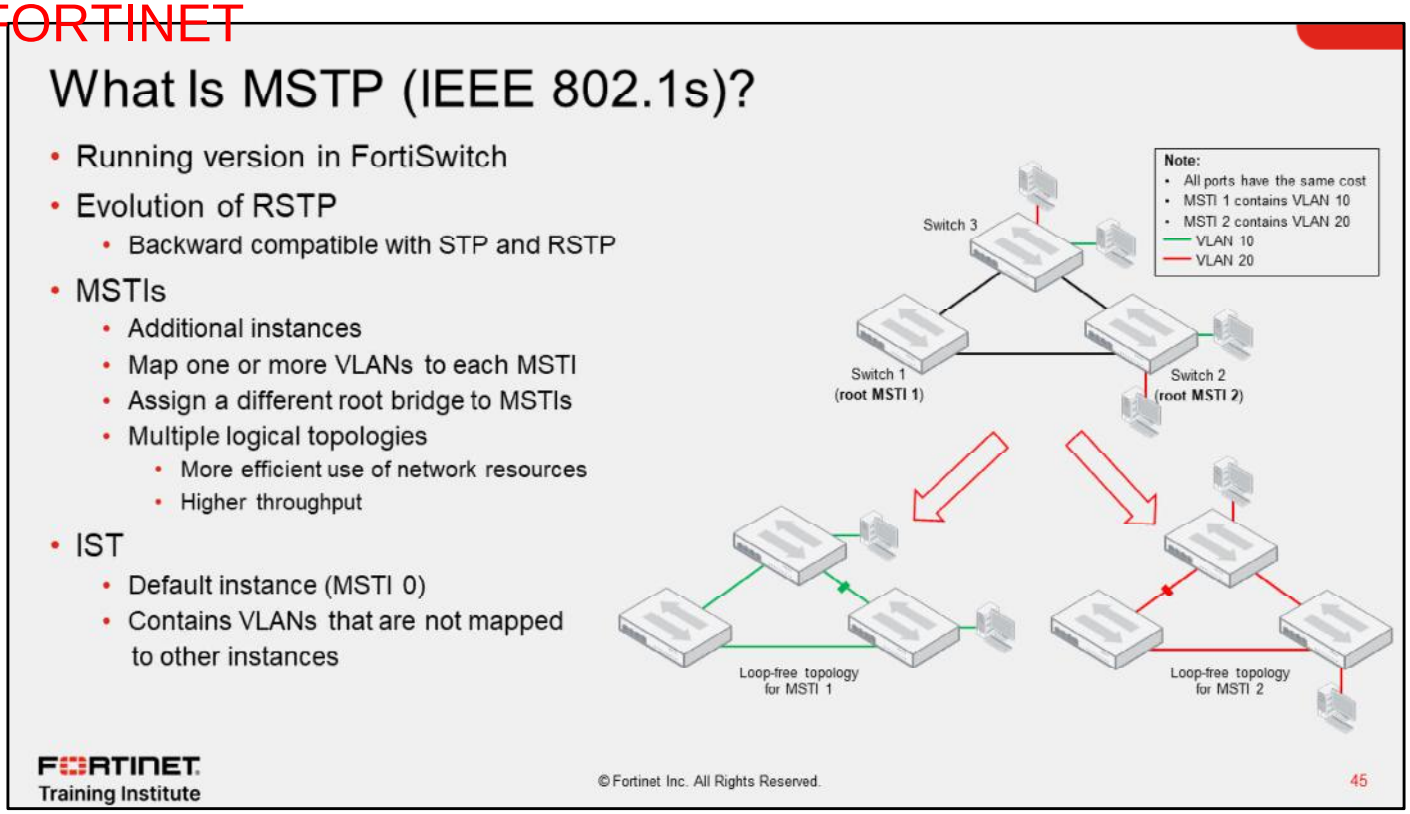


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in MSTP, you should be able to understand how FortiSwitch provides a loop-free topology on multiple instances, while being backward compatible to legacy and third-party switches using STP and RSTP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



STP and RSTP enable you to deploy redundant links in your LAN, while keeping the network loop free. Although preventing loops is critical, it also results in a surplus of resources that could otherwise be used to support a higher throughput. This is addressed by MSTP, which is the spanning tree version that runs on FortiSwitch.

MSTP, which is an evolution of RSTP and backward compatible with both of its predecessors, enables you to deploy Multiple Spanning Tree Instances (MSTIs), and then map one or more VLANs to each MSTI. Because you can also set a different root bridge for your MSTIs, the instances can converge to different logical topologies. The result is that the instances can use alternate paths that would otherwise be blocked for all VLANs if using STP or RSTP.

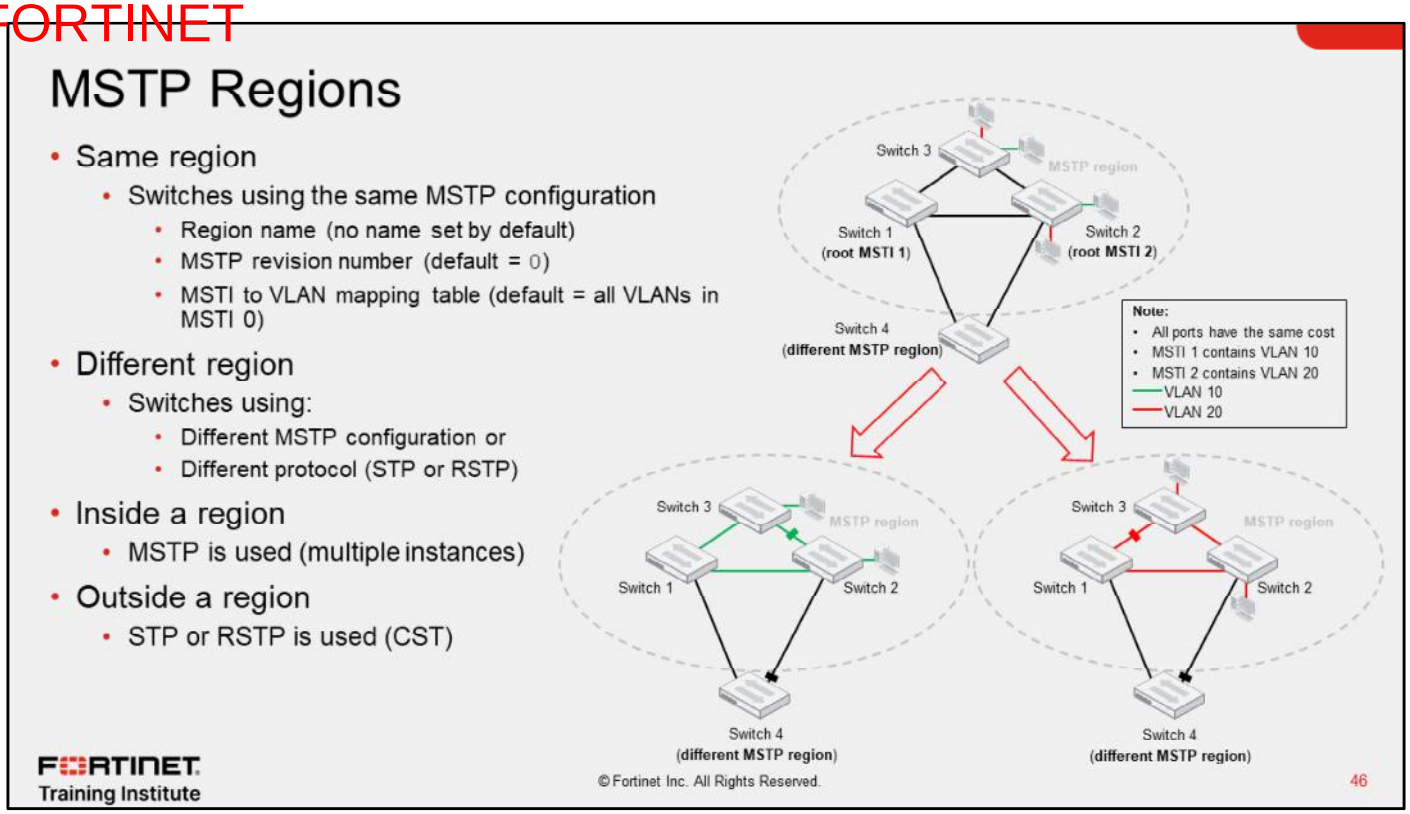
The physical topology shown on this slide has three interconnected switches and two VLANs. In STP and RSTP, the resulting loop-free topology would block the alternate path, which then forces traffic from both VLANs to be forwarded through the primary path, leaving the alternate path unused unless the primary fails.

But with MSTP, you can configure two MSTIs: MSTI 1 and MSTI 2, set a different root bridge for each instance, and then map one VLAN to each MSTI. The result is that MSTP calculates two different logical topologies, each using a different path to the root. The two different paths enable you to use all existing network links and therefore, make more efficient use of your network resources, while still keeping the network loop-free. Also, although in the example a single VLAN is mapped to an MSTI, you can actually map multiple VLANs to an MSTI. This enables you to map multiple VLANs to a reduced number of instances.

Finally, if you don’t create additional instances, there is a default instance called Internal Spanning Tree (IST), which is assigned to MSTI 0 on FortiSwitch, and that contains all the VLANs that haven’t been mapped to other instances.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



MSTP is backward compatible with STP and RSTP. When you configure your switch to use MSTP, the switch must first figure out what kind of protocol the adjacent switches are using. Switches that have the same MSTP configuration for the following attributes are placed in the same region:

- Region name: A name you assign to the region. By default, FortiSwitch does not assign a name.
- MSTP revision number: A number indicating your MSTP configuration version. The idea is to change the version number after you change the configuration. By default, FortiSwitch uses version 0.
- MSTI to VLAN mapping table: When you change the mapping, the table is updated. By default, all VLANs that haven't been placed in other MSTIs are placed in MSTI 0.

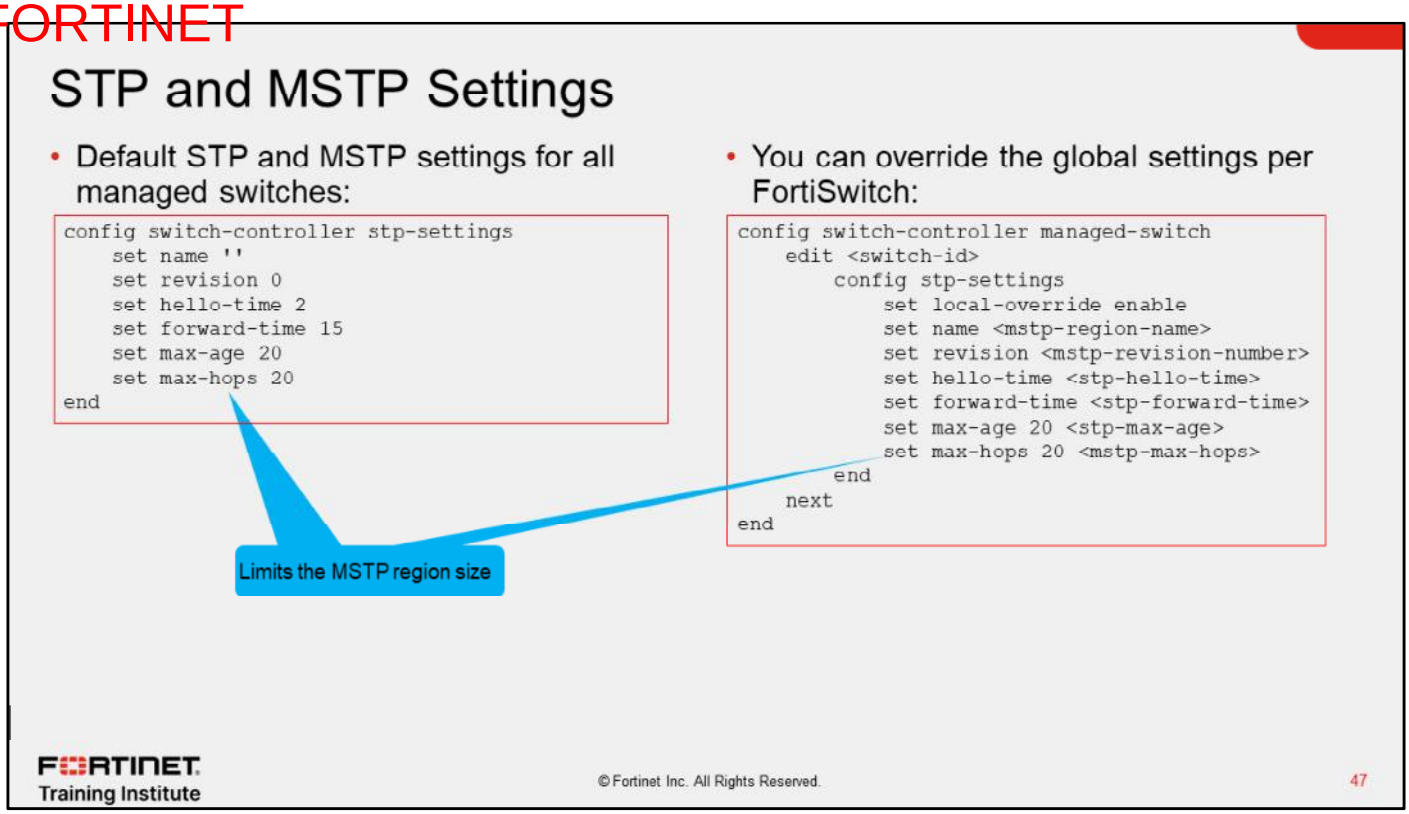
By contrast, switches that have different MSTP configurations or are using STP or RSTP, are seen as belonging to another region.

Within an MSTP region, MSTP is used to calculate the logical topology for the different instances. At the region boundary, and depending on the protocol used by the adjacent switch, MSTP switch ports use STP or RSTP to calculate a Common Spanning Tree (CST) topology that results in a loop-free topology for *all regions*. CST is just another way to call the single instance used by STP and RSTP to calculate a loop-free network for all VLANs.

The physical topology on this slide has four interconnected switches. Switch 4 belongs to a different region than the one where the other three switches operate. Within the region of the three switches, MSTP calculates two different topologies, one for each MSTI. However, at the region boundary, there is only one topology: the CST of the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



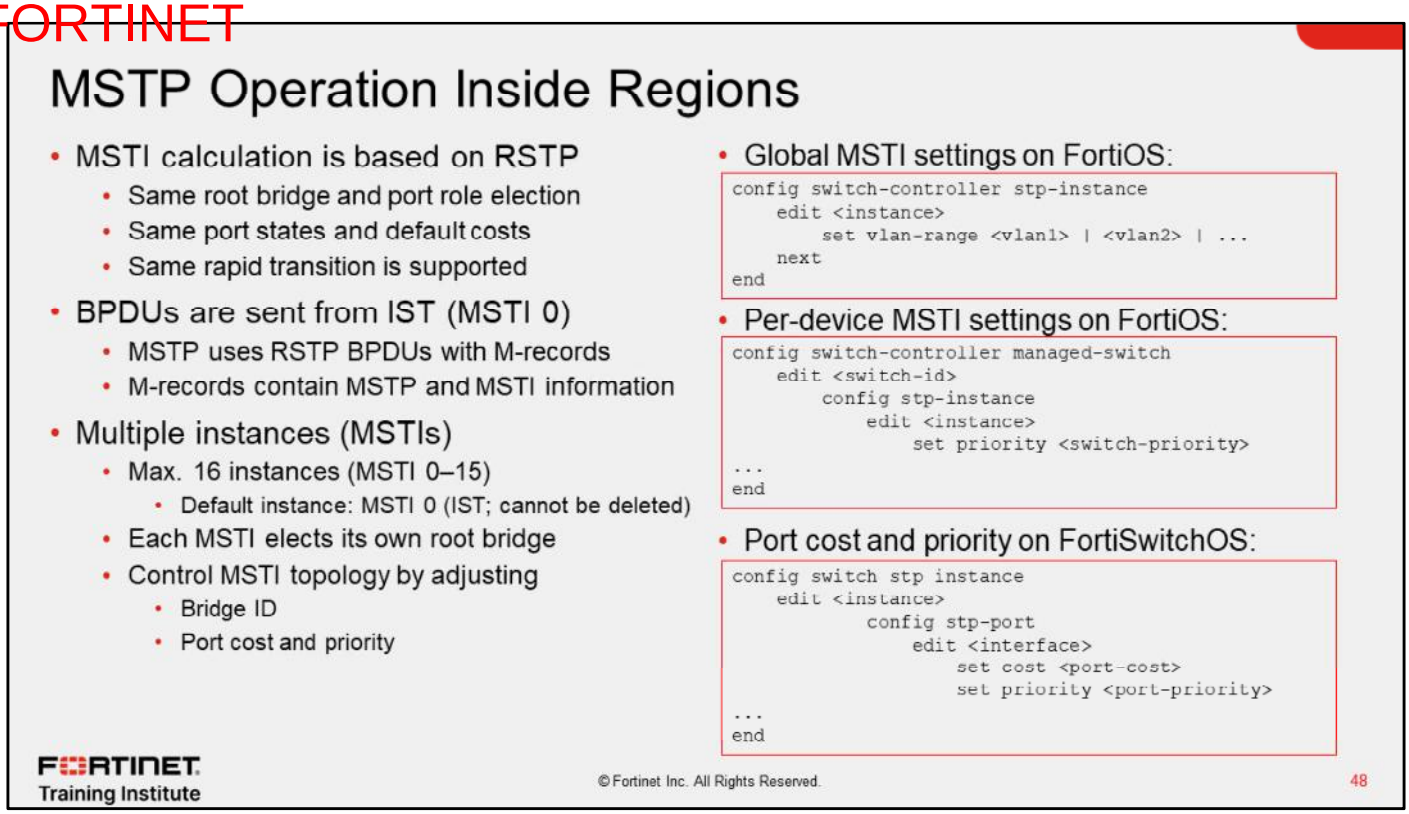
You can adjust the global STP and MSTP settings for all managed switches or override them on individual switches. This slide shows the FortiOS CLI commands you can use to adjust these settings either globally or per switch. Note that some settings are relevant only to STP, and others only to MSTP.

One setting that hasn't been discussed yet is `max-hops`. In an MSTP region, the `max-hops` setting defines the maximum number of hops that a BPDU sent by the root bridge can be forwarded in the region before it is considered expired and therefore, discarded by a receiving switch. When a non-root bridge receives the BPDU, the hop value in the BPDU decreases by 1 before the BPDU is forwarded to the next adjacent switch. If the hop value in a BPDU, is zero when a switch receives it, the switch discards the BPDU.

By default, `max-hops` is set to `20`. The goal of this setting is to limit the size of the MSTP region.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



MSTP calculates a loop-free topology for each instance, from the perspective of the root bridge on that instance.

Because MSTP is based on RSTP, the same rules used by RSTP for root bridge and port role election are used by MSTP on their instances. The port states and default port costs are also the same. In addition, instances also benefit from the rapid transition on full-duplex links and edge ports supported by RSTP.

The information of all instances is sent from the IST (MSTI 0) using MSTP BPDUs. The MSTP BPDUs are essentially RSTP BPDUs, except that they also include additional fields, called M-records, that carry MSTP-specific information, such as the MSTP region name, the configuration version, and the MSTI-to-VLAN mapping table digest. Note that BPDUs don't contain the actual MSTI-to-VLAN mapping table, but only a digest computed from it.

The M-records also carry MSTI-specific information, such as the local bridge ID, instance root bridge, and instance root path cost. The MSTI-specific information is then used by MSTP switches in a region to calculate topologies for each instance.

You can configure up to 16 instances on FortiSwitch (MSTI 0–15). MSTI 0 (IST) is the default instance and cannot be deleted. Each MSTI elects its own root bridge. The administrator can control the instance root bridge election by adjusting the bridge priority on that instance. The administrator can also control the role of a port by adjusting the port cost and priority on the instance.

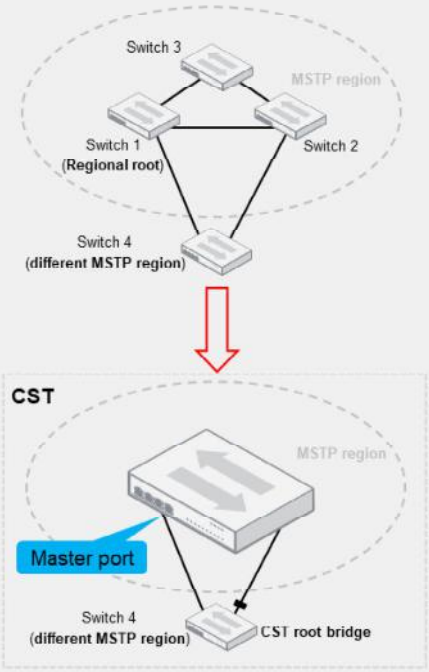
This slide shows the FortiOS CLI commands to create instances, set the bridge priority for an instance, and change the cost and priority on a port. Note that the port cost and port priority settings are available on the FortiSwitch CLI only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MSTP Operation Outside Regions

- A CST for all interconnected regions
  - Each region elects a regional root bridge on IST
  - A CST root bridge is elected
  - CST is built from the CST root bridge perspective
- For CST, boundary port uses:
  - RSTP if adjacent switch
    - Is an MSTP switch from another region or an RSTP switch
  - STP if adjacent switch uses STP
- Adjacent switch sees MSTP region as a single switch
  - Does not know or care about MSTIs in region
- Master port (new role)
  - Boundary port in MSTP region with best path to CST root bridge
  - Role is valid in outside region operation only



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

49

Switches that have different MSTP configurations or are using STP or RSTP, are seen as belonging to a different region. The interconnected regions then calculate a CST for the whole network.

Each region elects a regional root bridge on the IST (MSTI 0) that competes with other regional root bridges (different MSTP regions) or legacy switches (STP and RSTP switches) for the CST root bridge. The CST root bridge and port roles are elected using the same rules defined in STP and RSTP.

The switch port in an MSTP region that connects to another region is known as the boundary port and participates in the CST calculation. If the adjacent switch on a boundary port is an MSTP switch or an RSTP switch, both switches use RSTP for CST convergence. If the adjacent switch is an STP switch, STP is used.

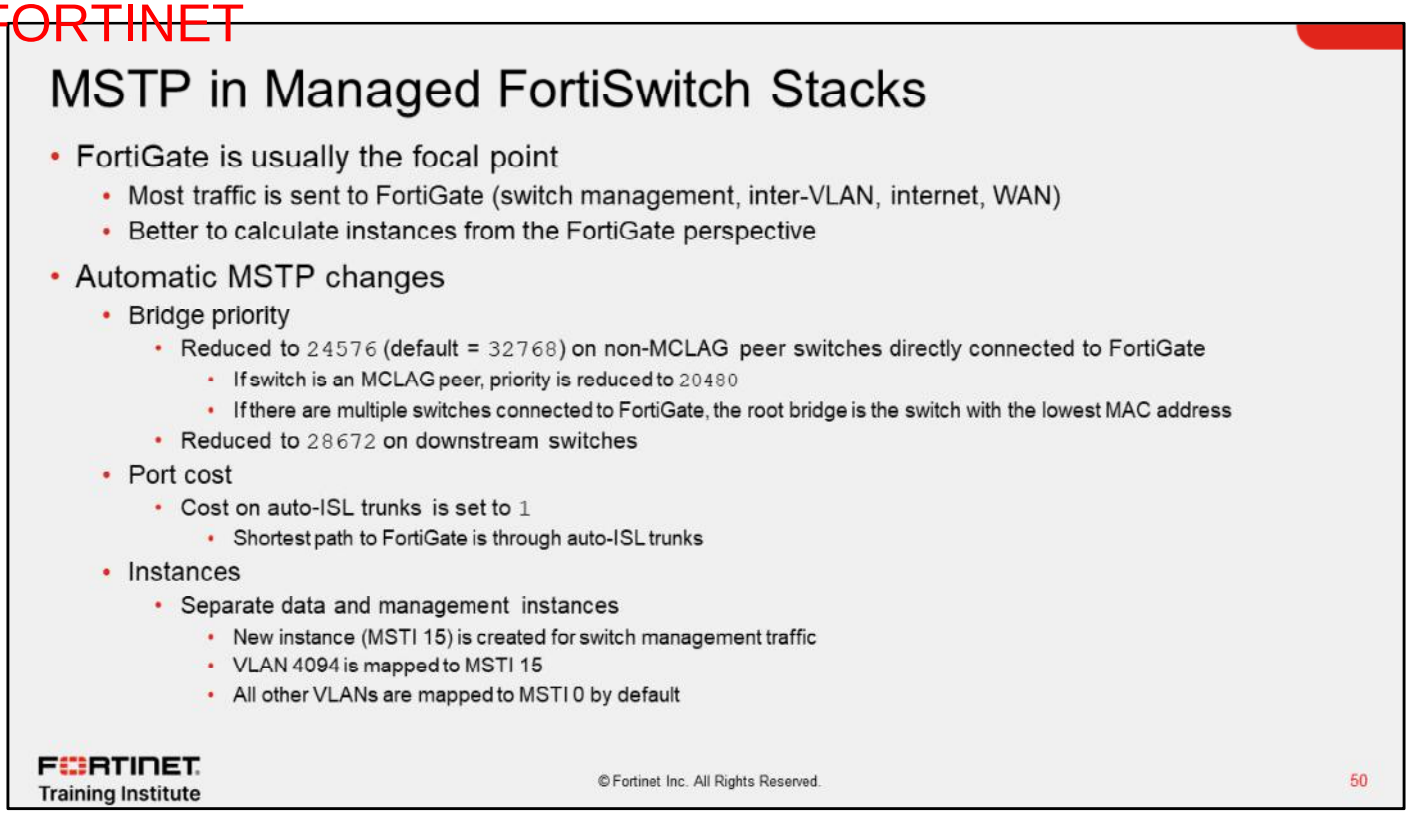
The MSTP region sees the adjacent switch connected to its boundary port as another region. By contrast, the adjacent switch (Switch 4 in the example) sees the whole MSTP region as a single switch. Switch 4 does not know anything about the internal instances on its neighbor, nor does it care. CST calculates a loop-free topology only on the links that connect the MSTP regions and legacy switches.

The example on this slide also shows a CST topology. A new port role, the *master port*, is also shown. The master port is the boundary port in a MSTP region that connects to the best path to the CST root bridge. A master port is like a root port, except that it connects to a different region. In the example shown on this slide, Switch 4 is the CST root bridge. The best path to the CST root bridge is over the link between Switch 1 and Switch 4. For this reason, the port on Switch 1 that connects to Switch 4 becomes the master port. Also, the alternate path between Switch 3 and Switch 4 is blocked.

Note that the master port role is seen when MSTP operates with outside regions only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In most managed switch deployments, FortiGate is the focal device in the network because most of the traffic is usually destined to FortiGate (switch management traffic), or networks behind FortiGate, such as the internet, VLANs, and the corporate WAN.

Given that FortiGate is the focal point in the network, it is convenient to have instances converged towards FortiGate by default. To accomplish this, the following MSTP settings are automatically changed in a managed FortiSwitch stack:

- Bridge priority: The bridge ID on non-MCLAG peer switches directly connected to the FortiGate FortiLink interface is reduced to 24576 (default priority is 32768). If the switch is an MCLAG peer, the bridge priority is reduced to 20480 instead. If there are multiple switches directly connected to FortiGate, the switch with the lowest MAC address becomes the root bridge. In addition, the bridge priority on downstream switches is reduced to 28672, so they don't become the root bridge.

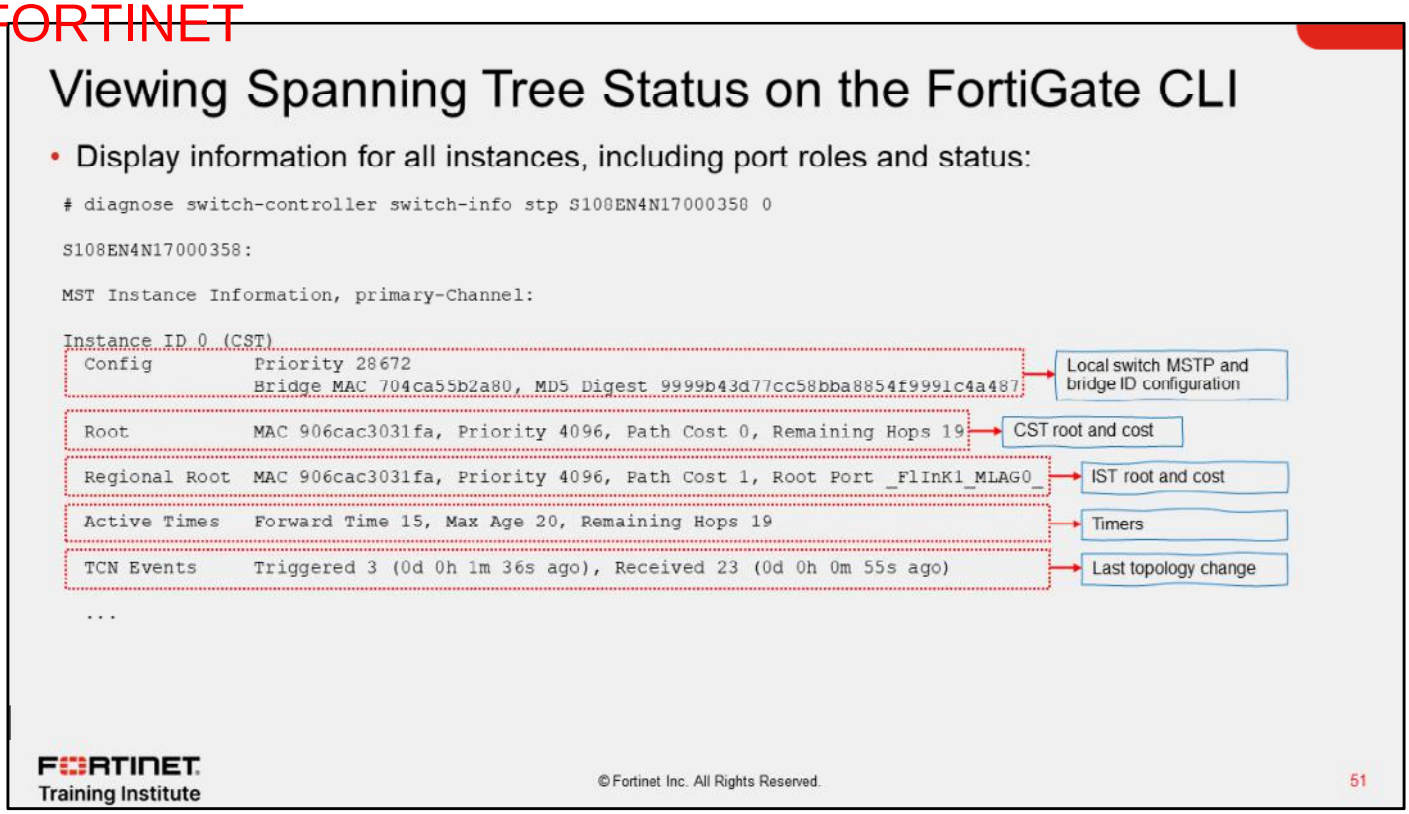
- Port cost: Auto-ISL trunks are assigned a cost of 1. Because auto-ISL trunks can be formed only when one of the adjacent switches is in managed mode, the trunk is likely to be the shortest path to FortiGate. Therefore, it is convenient to reduce its cost, so it becomes the preferred path to the root bridge.

- Instances: By default, only one instance (MSTI 0) is created on FortiSwitch. However, when FortiSwitch is authorized, another instance, MSTI 15, is created for management traffic. The instance is mapped to VLAN 4094, which is the switch management VLAN. Having separate instances for user and management traffic enables the administrator to adjust instance 0 settings, in case the user traffic must converge on a device that is not the switch controller, without impacting the management traffic on switches.

Note that the bridge priority and port cost changes are applied on both instances: 0 and 15.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



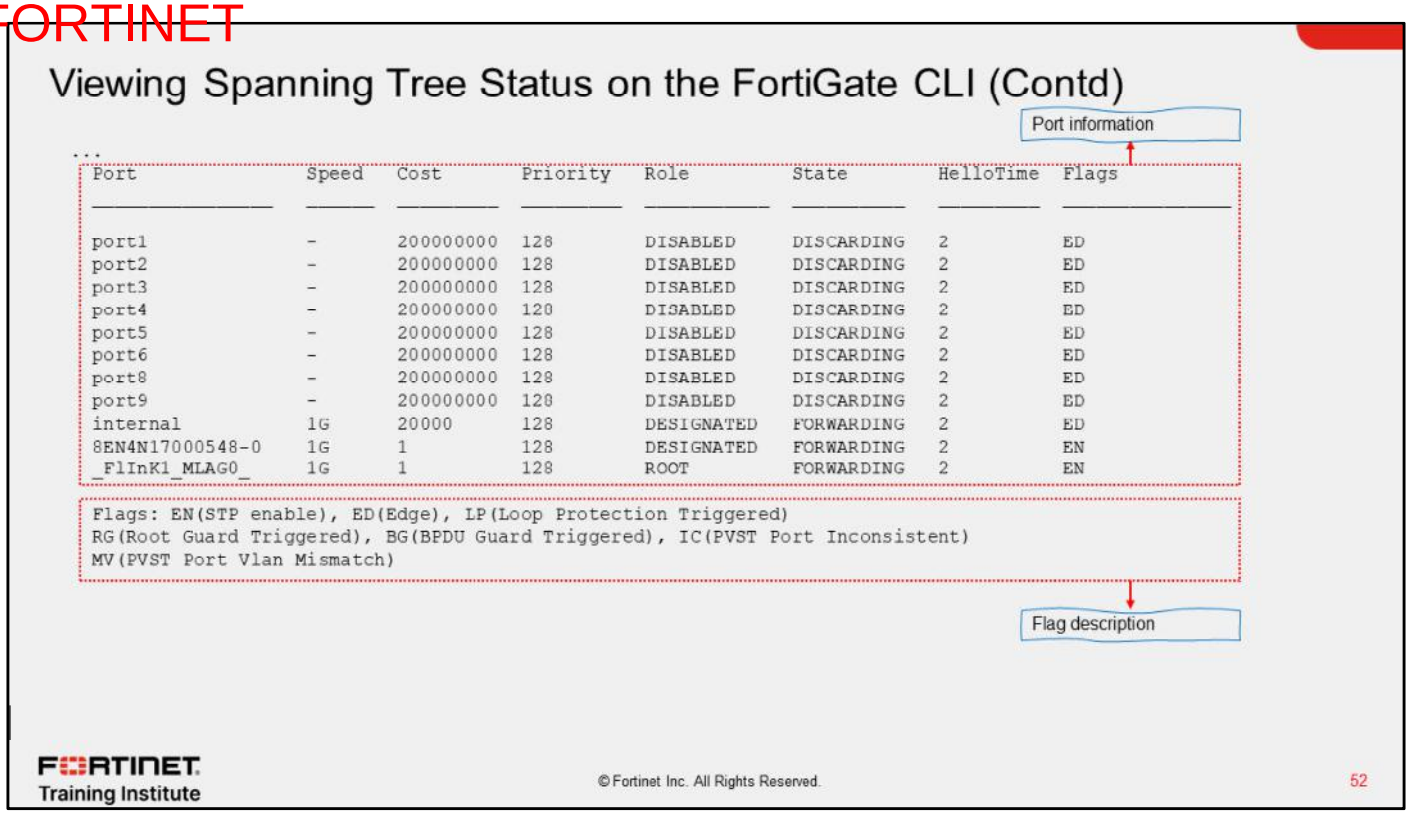
You can run the command shown on this slide to display spanning tree information for a specific instance on a managed switch. If you specify the instance number, FortiGate pulls information for all instances.

The example shown on this slide displays information for instance 0 only, also known as the CST when referring to MSTP operation outside a region, or IST when referring to MSTP operation inside a region. Note that the IST root is also the regional root. The regional root competes with other regional root bridges for the CST root bridge.

The output also displays the STP timers configured on the region. The timers are displayed for instance 0 only, because the other instances inherit the same timers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a continuation of the previous output. The output shows the port information section of the interfaces that participate in the MSTP instance. An interface, which can be an individual switch port or a trunk, participates in an instance when the interface belongs to one or more VLANs that are mapped to that instance.

For each port, the output indicates its cost, priority, role, state, and hello time. There is also a flag column that provides further information about the port, such as whether the port is configured as an edge port, or whether it triggered STP enhancement features, such as BPDU guard or loop protection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about MSTP operation is true?
✓A. MSTP is backward compatible with STP and RSTP.
B. MSTP supports a single instance only.

2. How do switches determine whether they belong to the same MSTP region?
✓A. By checking if they have the same region name, version, and MSTI to VLAN mapping table.
B. By exchanging LLDP frames.

3. Which statement about IST configuration on FortiSwitch is true?
✓A. It is the default instance (instance 0) for all VLANs.
B. It can be deleted.

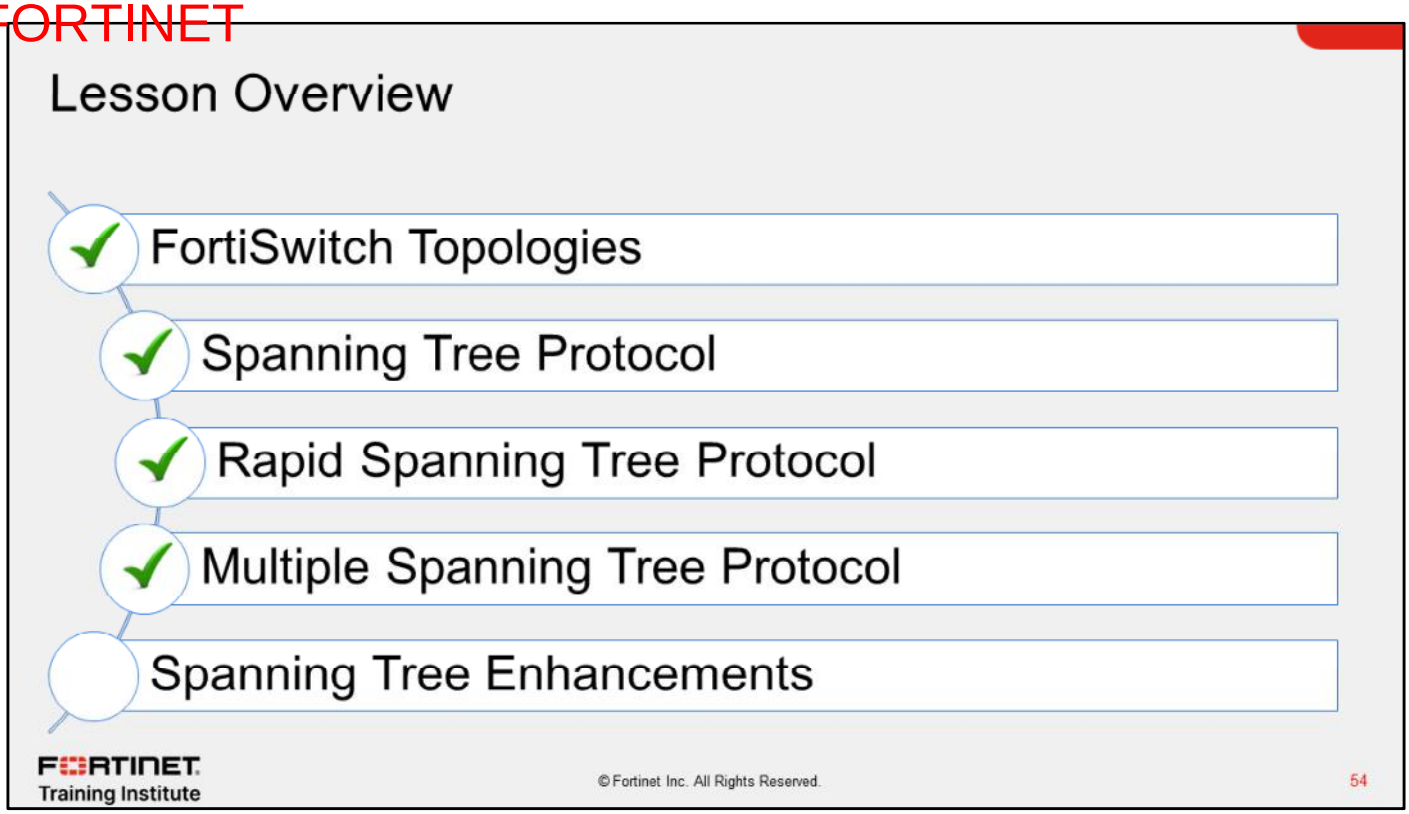
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

53

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

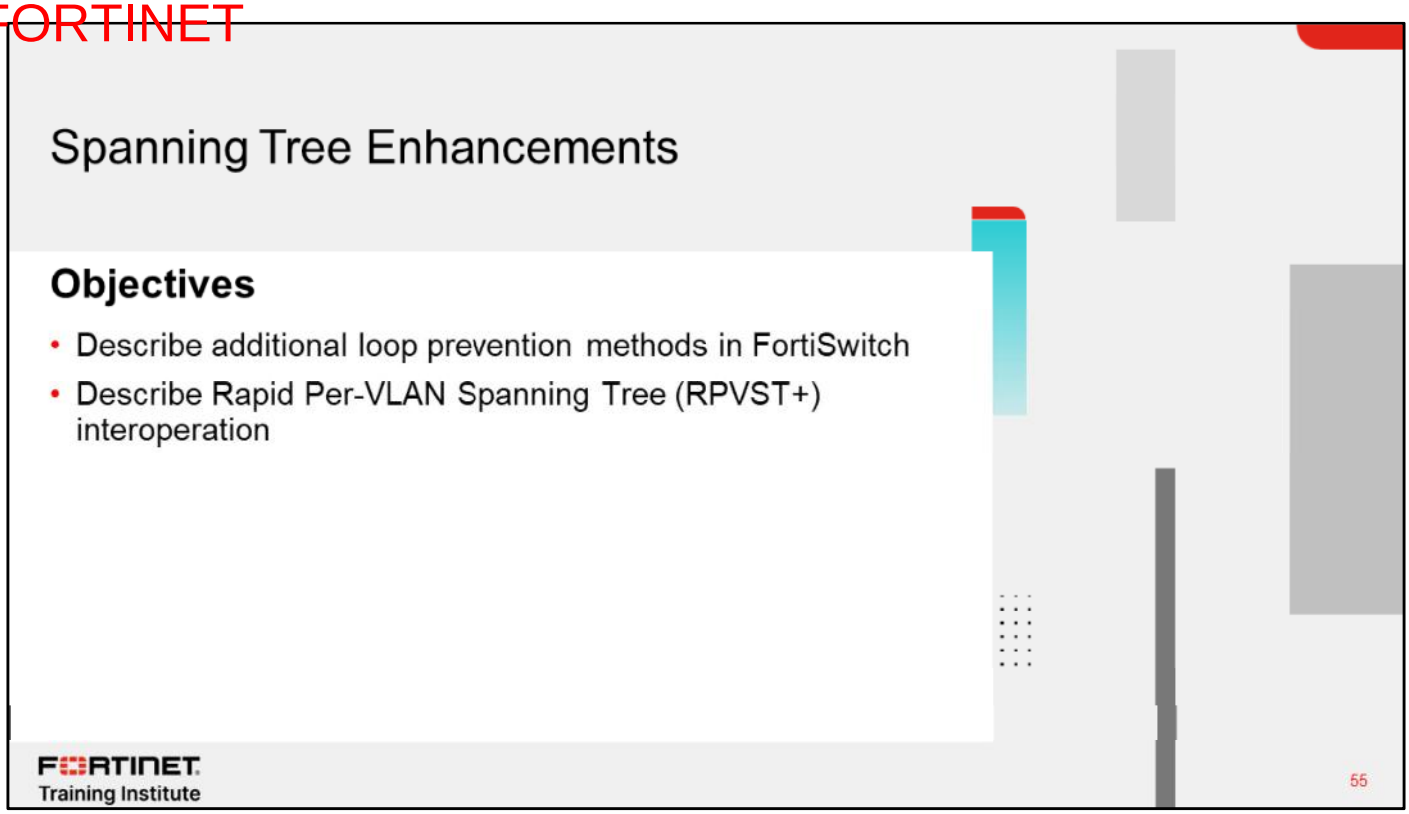


Good job! You now understand MSTP.

Now, you will learn about spanning tree enhancements.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

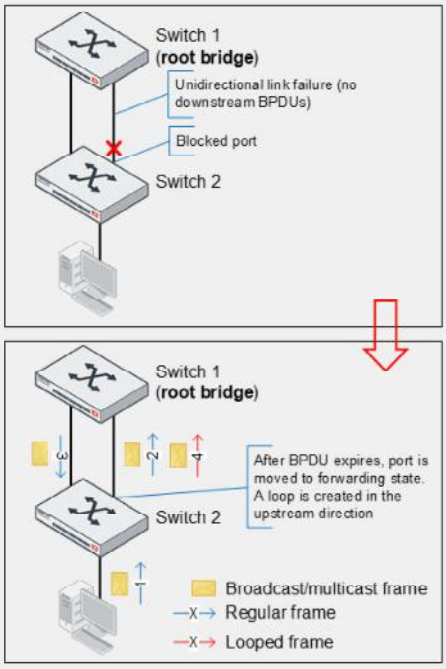
By demonstrating competence in spanning tree enhancements, you should be able to identify the additional loop prevention methods available in FortiSwitch that can operate in conjunction with MSTP to deliver a more robust loop-prevention solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Loop Protection

- Prevents loops undetected by STP
  - Blocked ports incorrectly move to forwarding state
  - Common case:
    - Unidirectional link failure
    - BPDUs expire on blocked port
    - Blocked port eventually starts forwarding traffic
    - Loop is created in opposite direction to link failure
- If loop protection is enabled on a port:
  - Blocked port stays in the blocking state if BPDUs are no longer received
  - No transition to forwarding state
- Loop protection is different than loop guard



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

56

Loop protection enables you to prevent loops that are caused by the transitioning to the forwarding state of blocked ports that connect to network segments where a loop may still be present.

After STP converges, only designated ports forward BPDUs down the spanning tree. Only non-designated ports—root and blocked ports—process incoming BPDUs. If a blocked port stops receiving BPDUs for a period longer than the max age time (20 seconds by default), the port transitions to the forwarding state. Note that in the case of RSTP and MSTP, the age time is three times the hello time (6 seconds if using default hello time), and the blocked port is classified as an alternate or backup port.

Now, suppose there is a unidirectional link failure that affects the BPDUs sent by a designated port to a blocked port. The opposite direction of the link, however, still works. After the blocked port transitions to the forwarding state, the port starts forwarding traffic in the working direction, which results in a broadcast storm due to the presence of a loop in that direction.

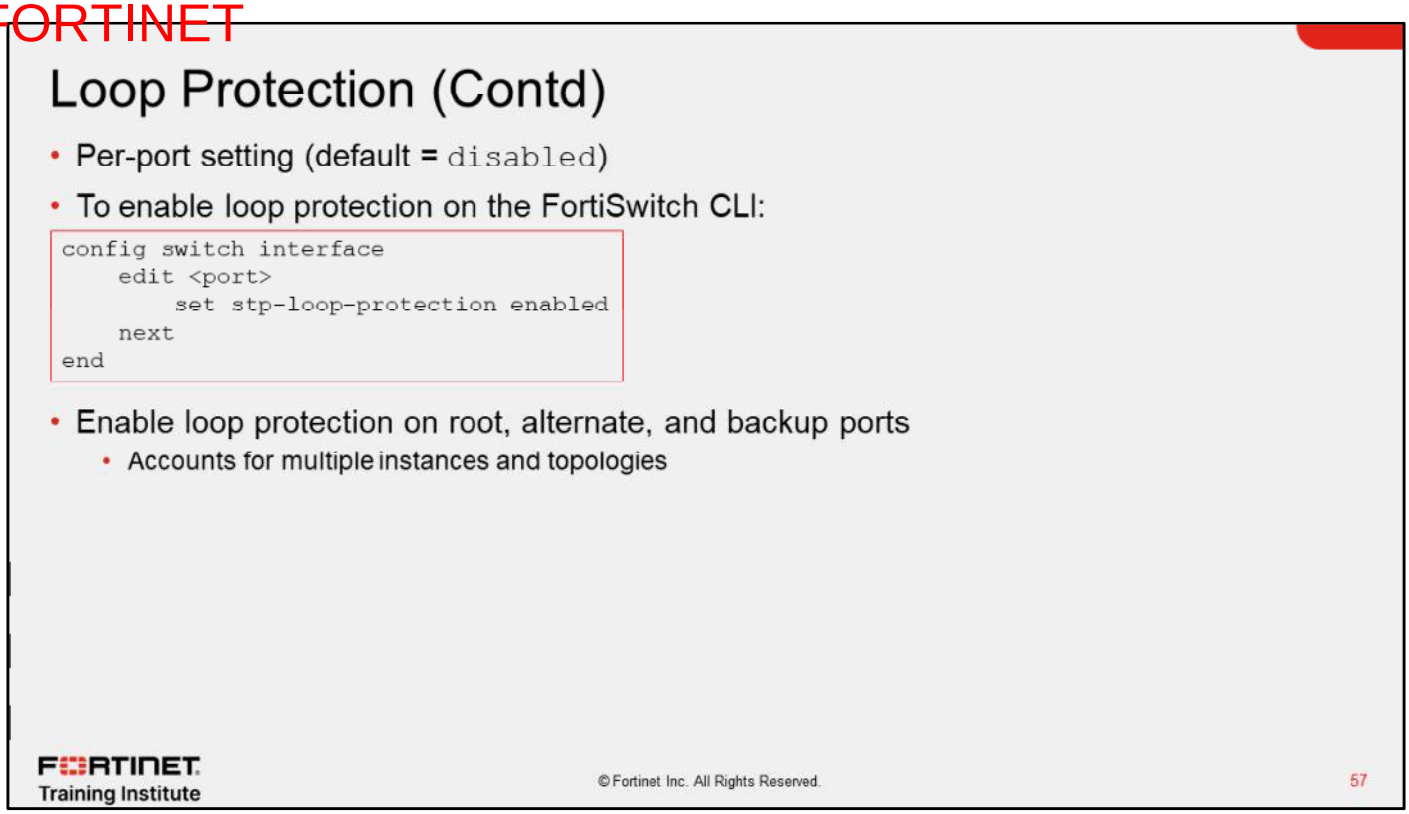
The example on this slide shows two switches interconnected through two links. The link on the right is the alternate link, and therefore is blocked by STP. If there is a unidirectional failure on the alternate link that affects downstream BPDUs, the blocked port on the alternate link eventually transitions to the forwarding state. As a result, broadcasts sent by the PC will loop in the network.

When you enable loop protection on a port, a blocked port is forced to remain in the blocking state, even if the port stops receiving BPDUs. The port does not transition to the forwarding state, nor does it forward user traffic.

Note that loop protection is different than loop guard. They both prevent loops, but they use different methods. You will learn more about loop guard in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Loop protection is a per-port setting, and it's disabled by default. This slide shows how to enable the setting on the FortiSwitch CLI.

If you want to use loop protection, it is recommended that you enable the feature on all root, alternate, and backup ports. The reason why you should also enable the setting on root ports is because you should consider the different topologies that MSTP can calculate when having multiple instances. For example, for one instance, a port can be a root port, but for another, an alternate or backup port. Loop protection will then be applied on the alternate or backup port on a per-instance basis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Root Guard

- Ignores superior BPDUs on a port
  - Prevents root port change and rerouting of traffic
    - Avoids service impact if new path is suboptimal
    - Prevents information theft by compromised endpoints
- Per-port setting (default = `disabled`)
- To enable root guard on the FortiGate GUI:

WiFi & Switch Controller > FortiSwitch Ports



- To enable root guard on the FortiGate CLI:

```
config switch-controller managed-switch
    edit <switch-id>
            edit <port>
                set stp-root-guard enabled
            next
    next
end
```

- Enable root guard on a port that connects to a switch with an unwanted path to root

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

58

When you enable root guard on a port, the port ignores superior BPDUs. The goal is to prevent a given port from becoming the root port, which would result in a topology change, and possible service disruption because the traffic could be rerouted through a suboptimal link. In addition, root guard can also protect the network from attacks from compromised endpoints that are used to capture traffic and steal information by generating rogue BPDUs.

Root guard is a per-port setting, and it's disabled by default. This slide shows how to enable the setting on the FortiGate GUI and CLI.

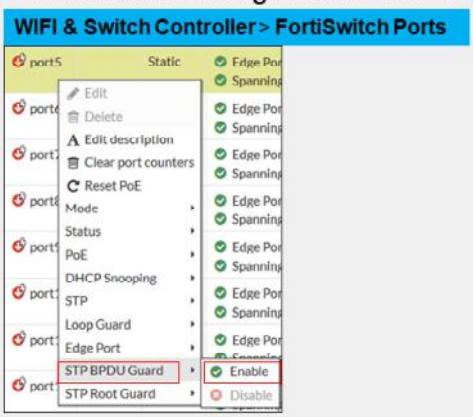
You usually want to enable root guard on a port that connects to a switch that should never become the best path to the root. For ports where you expect to connect only endpoints, it's often better to enable BPDU guard, which is also explained in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

BPDU Guard

- Blocks a port when it receives BPDUs
  - Port stays down for the time set in `stp-bpdu-guard-timeout` (default = 5 minutes)
- Per-port setting (default = `disabled`)
- To enable BPDU guard on the FortiGate GUI:



- To enable BPDU guard and change its timeout on the FortiGate CLI:

```
config switch-controller managed-switch
    edit <switch-id>
        edit <port>
            set stp-bpdu-guard enabled
            set stp-bpdu-guard-timeout <mins>
        next
    next
end
```

- To reset the status of a port on the FortiGate CLI:

```
# execute switch-controller switch-action bpdu-guard
reset <switch-id> <port>
```

- Enable BPDU guard on ports that connect to endpoints
  - Endpoints shouldn't send BPDUs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

59

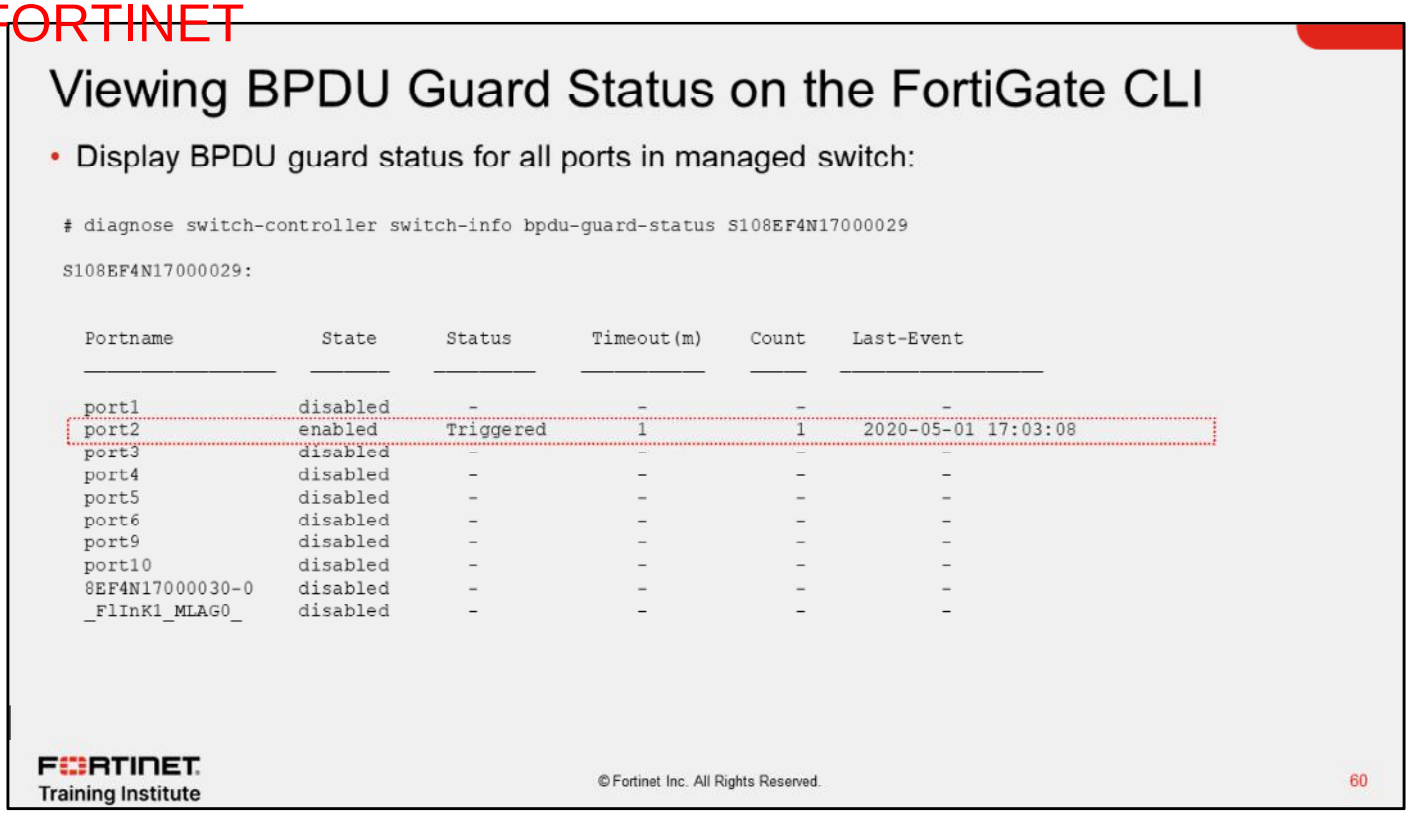
When you enable BPDU guard on a port, the port is shut down for the time configured in the `stp-bpdu-guard-timeout` setting—five minutes by default—when the port receives any BPDUs. After the BPDU guard timeout is reached, the port is brought back up, but will be shut down again if more BPDUs are received.

BPDU guard is a per-port setting, and it's disabled by default. This slide shows how to enable the setting on the FortiGate GUI and CLI, and how to change the BPDU guard timeout on the FortiGate CLI. The administrator can also reset the status of ports that are brought down by BPDU guard, by running the FortiOS `execute` command shown on this slide.

Most of the time, you want to enable BPDU guard on a port that connects to an endpoint. Endpoints are not expected to send BPDUs. If they do, it could be an indication of compromise.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can run the command shown on this slide to display the BPDU guard status for all ports on a managed switch.

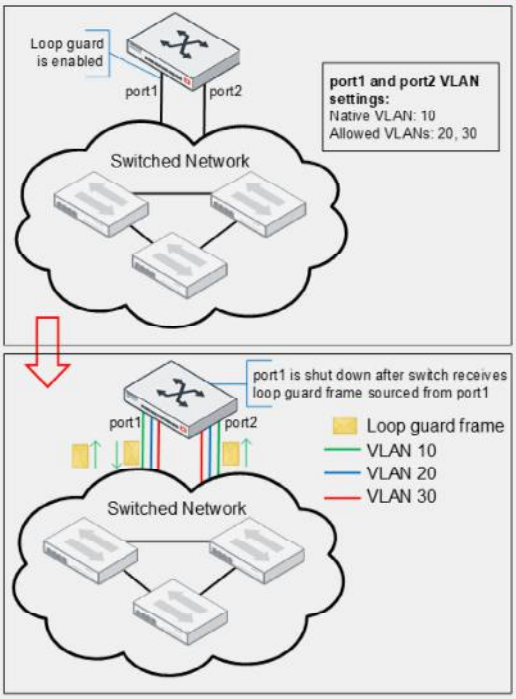
The example shown on this slide indicates that BPDU guard is enabled and triggered on `port2`. The output also shows the timestamp of the last trigger event, the total number of triggered events, as well as the configured timeout.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Loop Guard

- Also prevents loops missed by STP
  - Designed to work with STP, not to replace STP
- If loop guard is enabled on a port
  - Switch broadcasts loop guard frame on the native VLAN
  - If loop guard frame is received on sender switch
    - Port is shut down for the time set in `loop-guard-timeout` (default = `45` mins)
- Set MAC move threshold to detect loops on non-native VLANs
  - Switch monitors MAC address flapping events
  - Port is shut down if:
    - Number of flapped MAC addresses exceed the threshold within a second and for 6 consecutive seconds
- Loop guard can detect more loop cases than loop protection



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

61

Loop guard is another loop prevention feature. However, unlike loop protection, root guard, and BPDU guard, loop guard does not rely on BPDUs and the port state. Instead, loop guard works by periodically broadcasting loop guard frames on the native VLAN of a port. A loop is detected when the same loop guard frame is received on the sender switch, which is followed by the port getting shut down for the time specified in the `loop-guard-timeout` setting (45 minutes by default).

The original loop guard implementation didn't account for loops on VLANs, other than the native VLAN. For this reason, the loop guard feature was improved to include the *MAC move* option, which instructs the switch to also monitor for repeated MAC address flapping events, which are likely caused by a loop. To enable MAC move, you define a MAC move threshold other than zero. The threshold refers to the minimum number of MAC addresses that must flap between ports within a second. If the threshold is reached for six consecutive seconds, loop guard is triggered, and the port is shut down.

This slide shows port1 and port2 on FortiSwitch connected to a switched network. Both ports are assigned VLAN 10 as their native VLAN, and allow VLANs 20 and 30. Because loop guard is enabled on port1, FortiSwitch broadcasts loop guard frames on VLAN 10 on that port. FortiSwitch then shuts down port1 if it receives a loop guard frame sourced from port1 on either port1 or port2. If you also want to detect loops on VLANs 20 and 30, you must also enable MAC move on port1.

Both loop guard and loop protection detect loops in your network. However, because loop guard does not rely on STP, it can detect more loop cases than loop protection. For example, if you disconnect the uplink on port2 in the topology, loop guard will still detect the loop on port1, but loop protection will not.

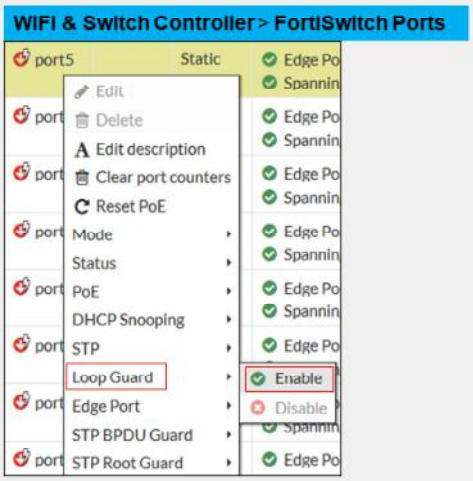
Note that loop guard is designed to work with STP, rather than replace it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Loop Guard (Contd)

- Per-port setting (default = `disabled`)
- To enable loop guard on the FortiGate GUI:



- To enable loop guard on the FortiGate CLI:

```
config switch-controller managed-switch
    edit <switch-id>
            edit <port>
                set loop-guard enabled
                set loop-guard-timeout <mins>
            next
    next
end
```

- To enable MAC move on the FortiSwitch CLI:

```
config switch interface
    edit <port>
        set loop-guard-mac-move-threshold <0-100>
    next
end
```

- To reset the status of a port on the FortiGate CLI:

```
# execute switch-controller switch-action loop-
guard reset <switch-id> <port>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

62

Loop guard is a per-port setting, and it's disabled by default. This slide shows how to enable the setting on the FortiGate GUI and CLI.

If you also want to enable MAC move, you must configure the setting directly on FortiSwitch. Note that the lower you set the MAC move threshold to, the higher the chances are of you getting false positive for loops.

The administrator can also reset the status of ports that are brought down by loop guard, by running the FortiOS `execute` command shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Loop Guard Status on the FortiGate CLI

- Display loop guard status for all ports in managed switch:

```
# diagnose switch-controller switch-info loop-guard S108EF4N17000029

S108EF4N17000029:

  Portname            State     Status      Timeout(m)   MAC-Move   Count   Last-Event
  ________________    _______   _________   __________   ________   _____   ___________________
  port1               enabled   Triggered   2            0          1       2021-02-19 15:50:35
  port2               disabled  -           -            -          -       -
  port3               disabled  -           -            -          -       -
  port4               disabled  -           -            -          -       -
  port5               disabled  -           -            -          -       -
  port6               disabled  -           -            -          -       -
  port9               disabled  -           -            -          -       -
  port10              disabled  -           -            -          -       -
  8EF4N17000030-0     disabled  -           -            -          -       -
  _FlInK1_MLAG0_      disabled  -           -            -          -       -
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

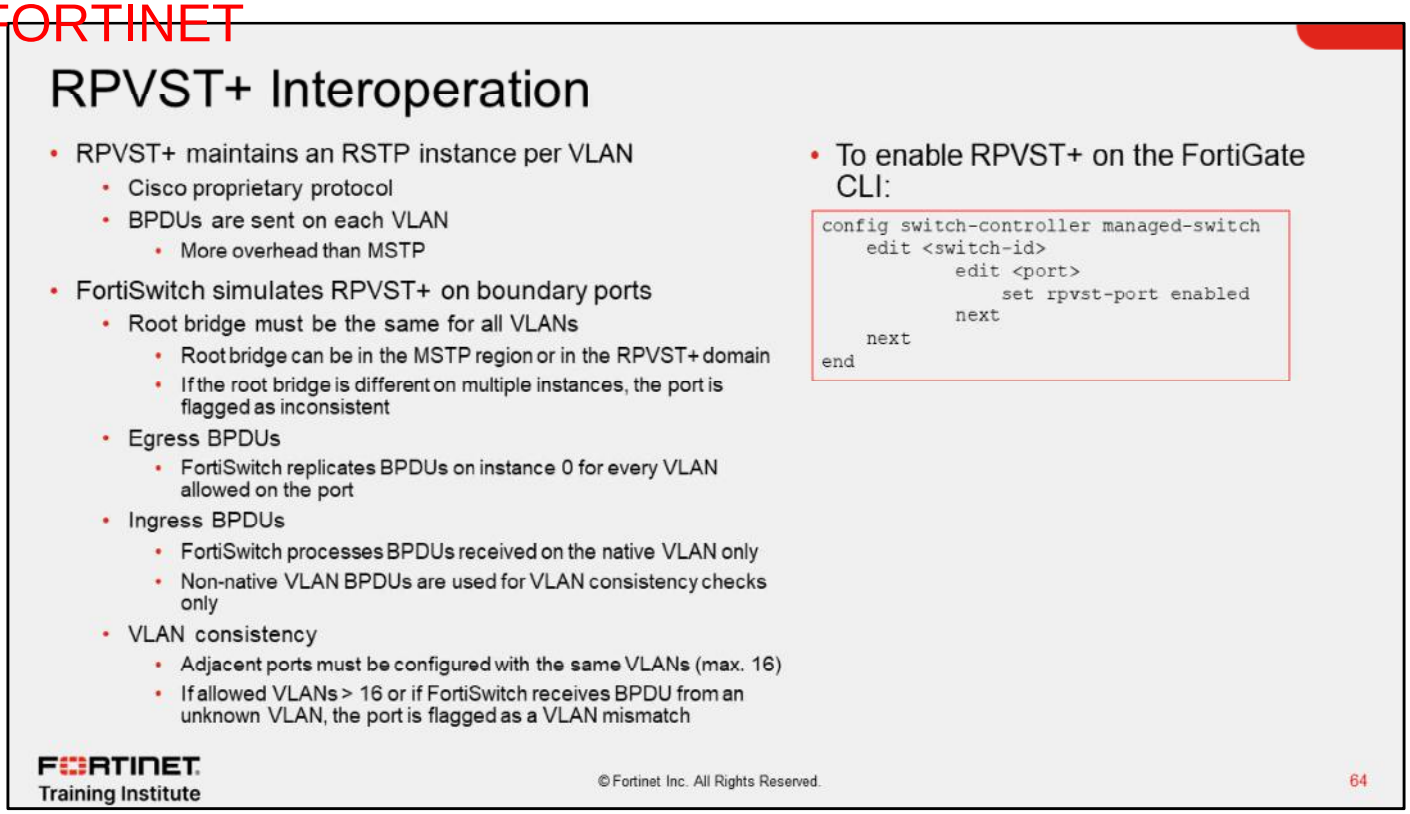
63

You can run the command shown on this slide to display the loop guard status for all ports on a managed switch.

The example shown on this slide indicates that loop guard is enabled and triggered on `port1`. The output also shows the timestamp of the last trigger event, the total number of triggered events, as well as the configured timeout. A value of zero in the `MAC-move` column indicates that the MAC move feature is not enabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



RPVST+ is a Cisco proprietary protocol that calculates a separate RSTP topology for every VLAN created on the switch. RPVST+ does this by sending separate BPDUs for each VLAN, with the BPDUs tagged with the VLAN IDs they correspond to. When compared to MSTP, MSTP can also calculate a separate RSTP topology for every VLAN in the region, except the information for all instances is included in the BPDUs sent from instance 0. In other words, MSTP can offer the same as RPVST+, but with much less overhead.

FortiSwitch can interoperate with RPVST+ switches. To achieve this, FortiSwitch pretends to be an RPVST+ switch at the boundary ports that connect the FortiSwitch MSTP region to the adjacent RPVST+ switch. RPVST+ interoperation works as follows:

- No support for a different root bridge per VLAN. The administrator must adjust the bridge priority setting on the switches to ensure that the root bridge is the same switch for all VLANs. The root bridge can be in the MSTP region or in the RPVST+ domain, but it must be the same for all VLANs on both switches. If FortiSwitch detects that the root bridge is different on multiple instances, the port is flagged as *inconsistent*.

- FortiSwitch simulates an RPVST+ switch by replicating the BPDUs on instance 0 for every VLAN ID allowed in the port. FortiSwitch processes BPDUs received on the native VLAN only. BPDUs from other VLANs are used only for VLAN consistency checks.

- VLANs on the adjacent ports must be consistent and cannot exceed 16 VLANs. If you allow more than 16 VLANs on a port, or if FortiSwitch receives BPDUs on a VLAN that is not allowed on the port, the port is flagged as a *VLAN mismatch*.

RPVST+ is a per-port setting, and is disabled by default. This slide shows how to enable the setting on the FortiGate CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about loop protection is true?
   - ✓ A. It monitors incoming BPDUs on blocked ports.
   - B. It can be enabled on FortiGate under the `switch-controller managed-switch` sub-section.

2. Which feature prevents a port from becoming a root port?
   - A. Loop guard
   - ✓ B. Root guard

3. Which is a limitation of the RPVST+ feature?
   - A. It cannot be enabled on FortiGate.
   - ✓ B. It supports a maximum of 16 VLANs.

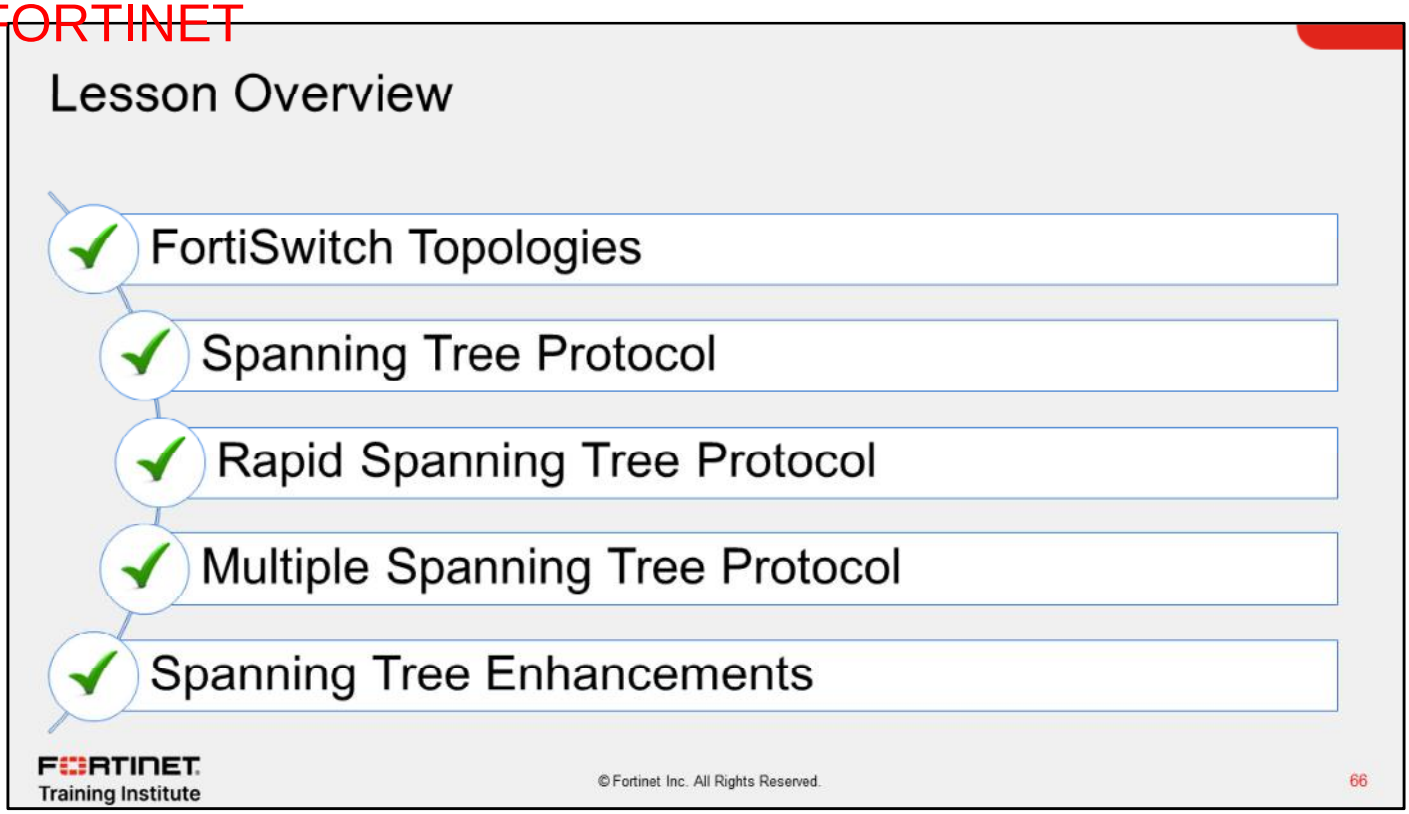
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

65

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

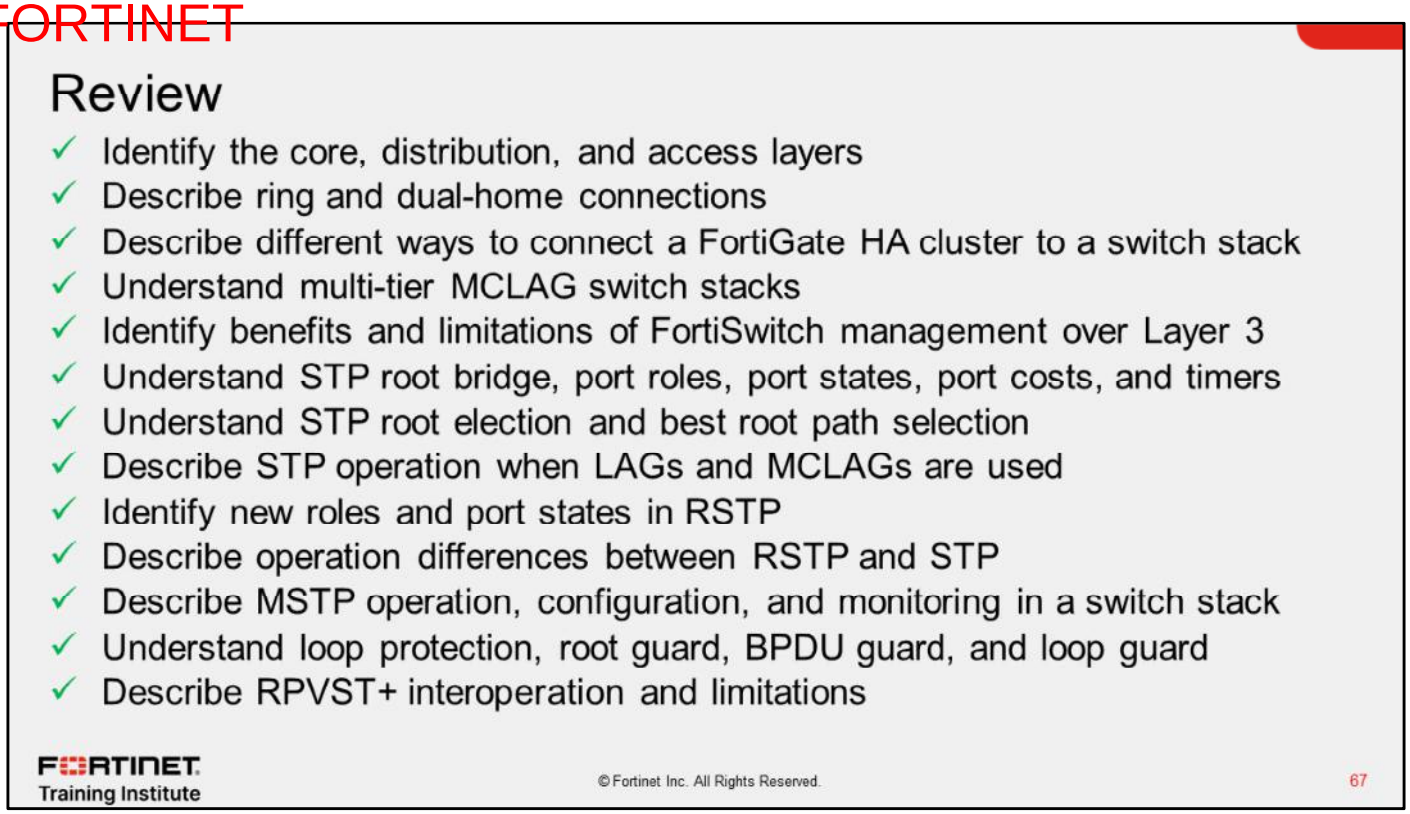


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

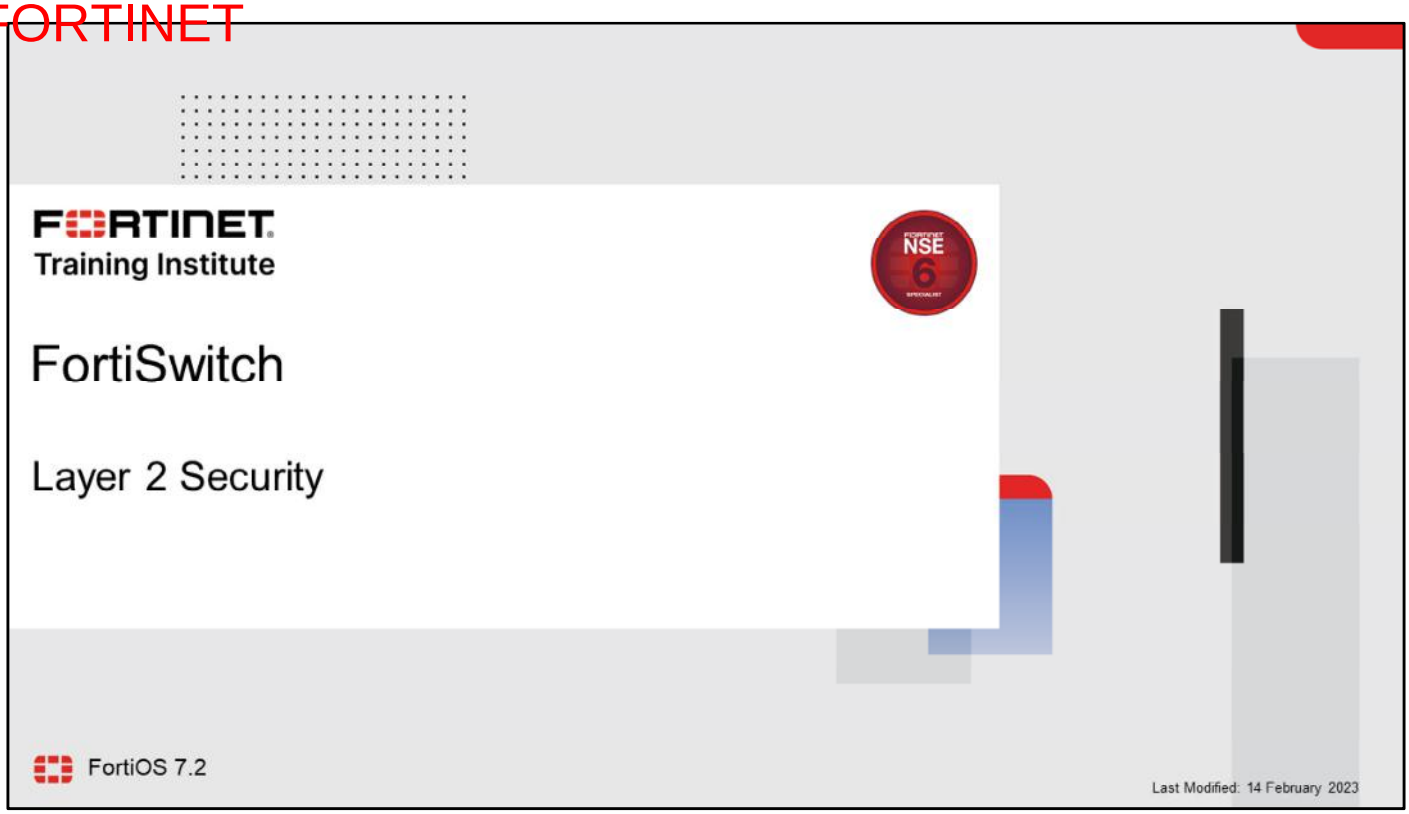


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the most common FortiSwitch deployments, and how spanning tree and other loop prevention methods can be used to ensure a loop-free topology.

Vouchers & Dumps are Available | WhatsApp +201224560923

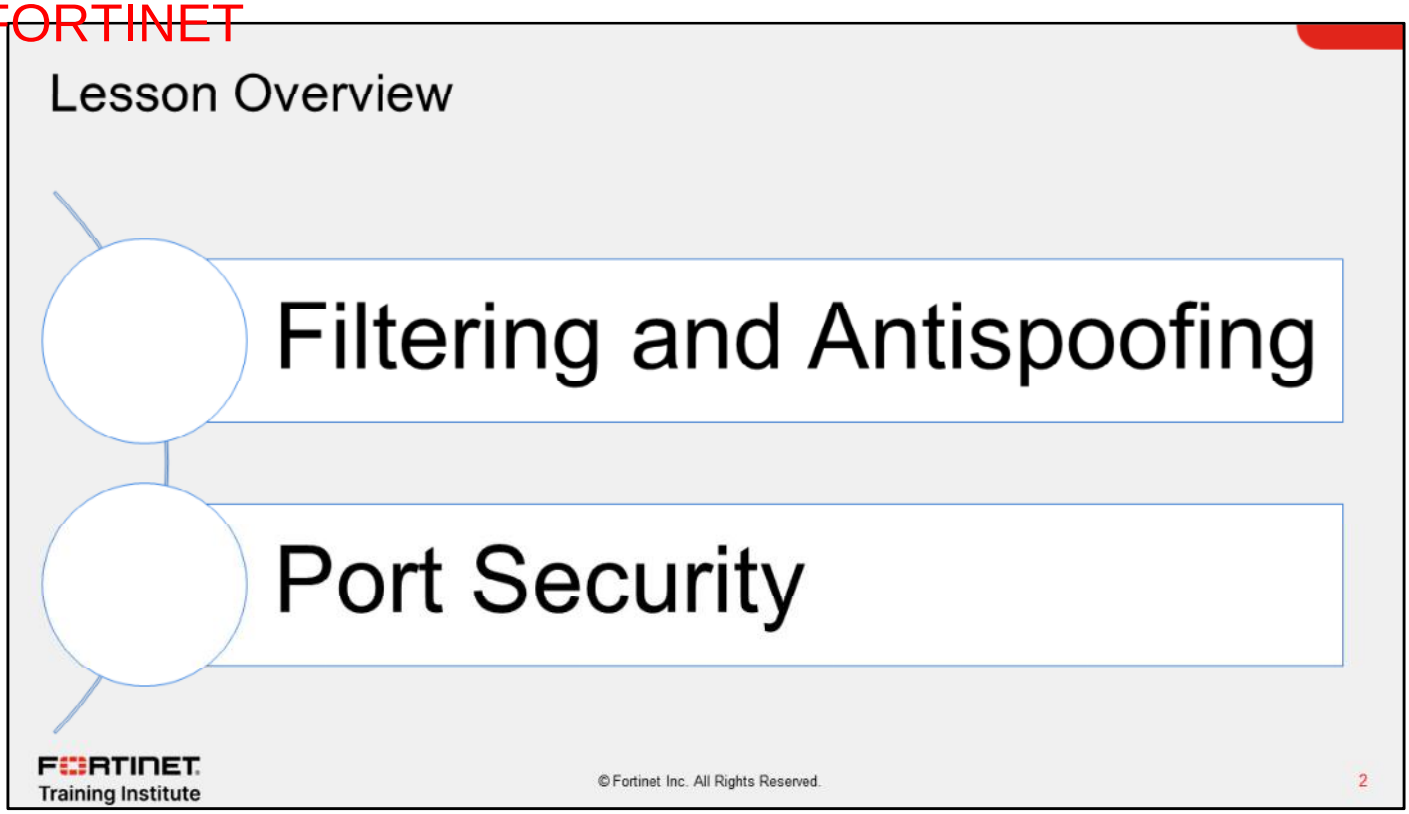
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the different security features you can deploy on FortiSwitch to protect your network at Layer 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

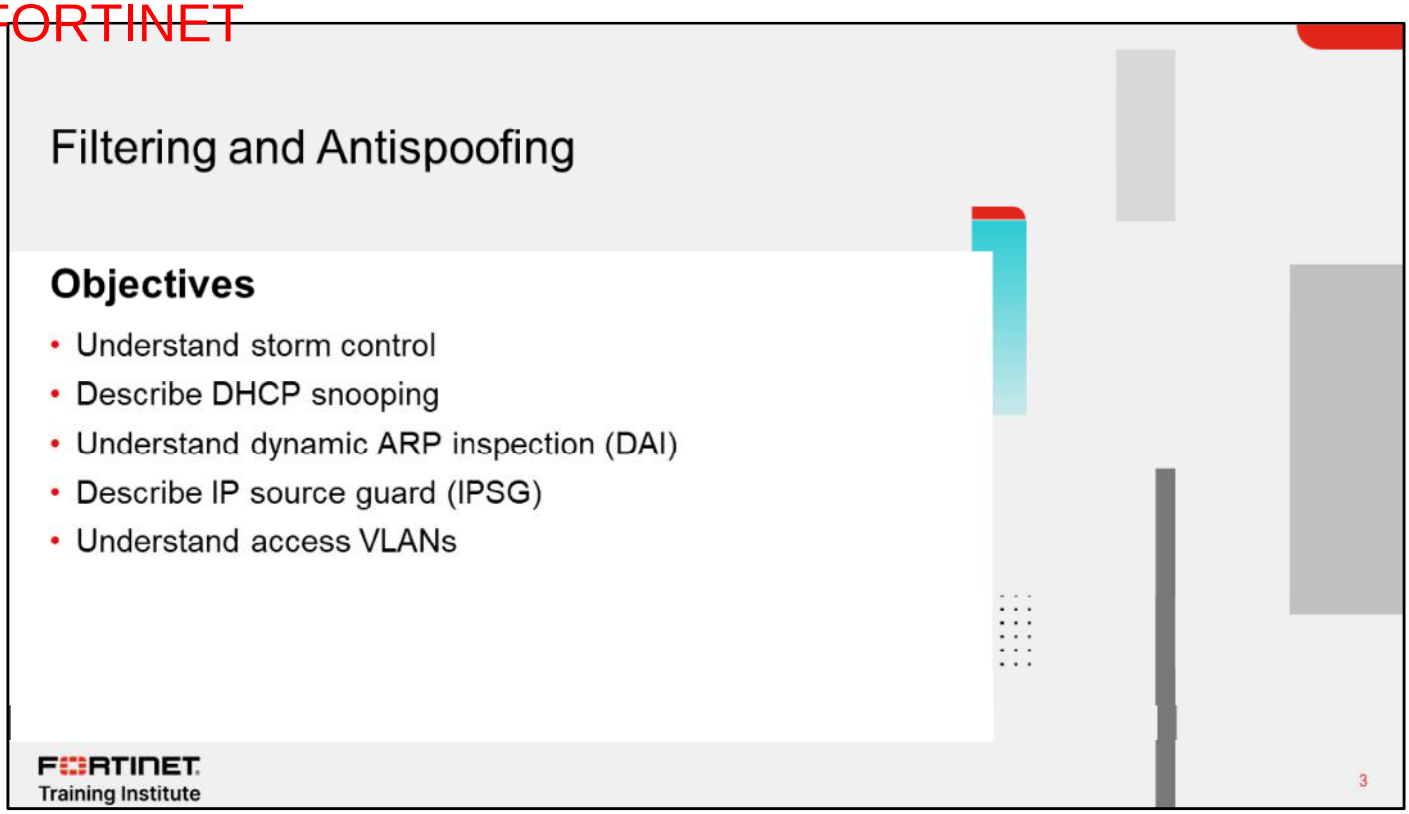
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

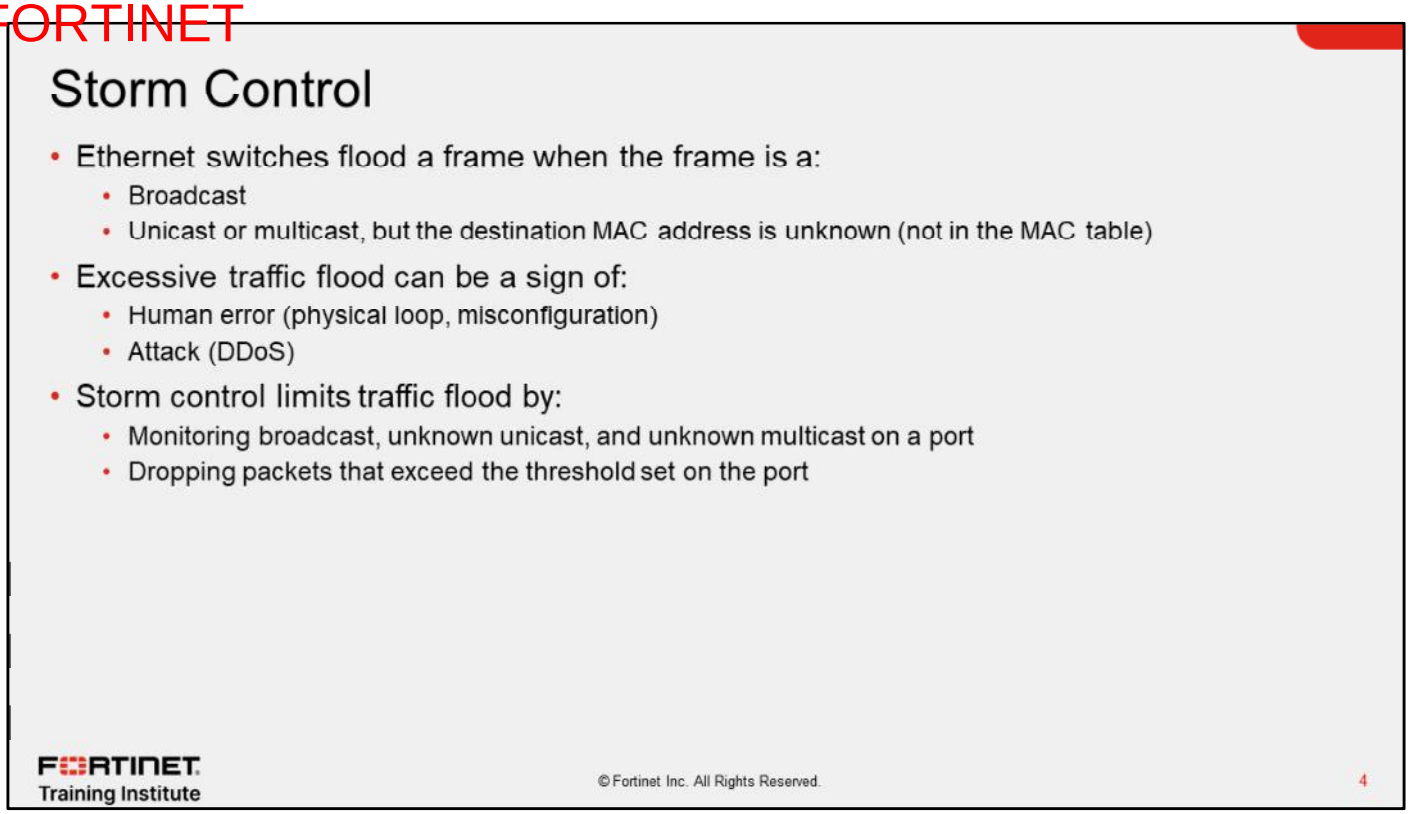


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the filtering and antispoofing features supported by FortiSwitch, you should be able to understand how to filter unwanted traffic in your network and prevent spoofing attacks at the switch level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When an Ethernet switch processes traffic, the switch floods a frame in the following cases:

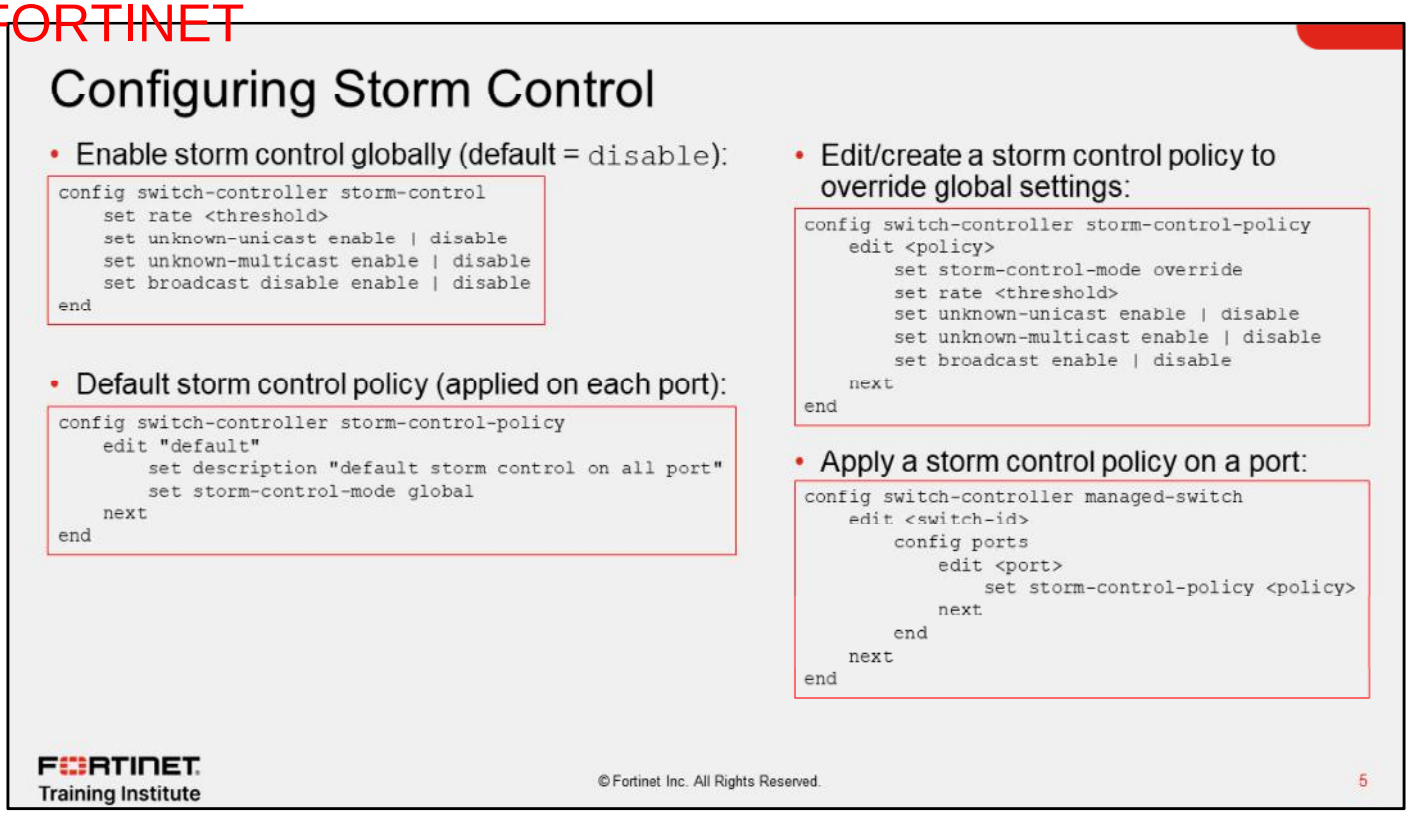
- The frame is a broadcast frame. All bytes on the destination MAC address are set to `FF`.
- The frame is a unicast frame, and the destination MAC address is unknown—not in the MAC address table. This usually happens when the switch hasn't learned the MAC address of a device yet or when the entry expired.
- The frame is a multicast frame, and the destination MAC address is unknown. The destination MAC address of a multicast frame is generated by the sender based on the target multicast group. Unless a feature like IGMP snooping is used, switches also flood multicast frames because the destination MAC address is unknown to the switch. You will learn more about IGMP snooping in another lesson.

Broadcast, unknown unicast, and unknown multicast are common in stable networks because they are used by discovery and provisioning services, and because dynamic entries in a MAC address table can expire. However, an excessive amount of this traffic can also be an indication of human error (physical loop, misconfiguration) or an attack (DDoS), which can result in performance degradation or even service disruption.

Storm control enables you to protect your network from excessive traffic flood. You can assign a threshold that controls the maximum number of broadcast, unknown unicast, and unknown multicast packets that are allowed in a second on a port. Packets exceeding the threshold rate set on the port are dropped by the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Storm control for all traffic flood types—broadcast, unknown unicast, and unknown multicast—is disabled by default. You can either enable storm control globally or override the global settings on a port. When you configure storm control, you set a threshold and enable the traffic flood types to monitor.

This slide shows how to enable storm control globally. When you enable storm control globally, the configured threshold is enforced independently on each port of all managed switches. For example, a threshold of 500 means that a switch drops the monitored flood traffic on a port when the rate exceeds 500 frames per second on that port.

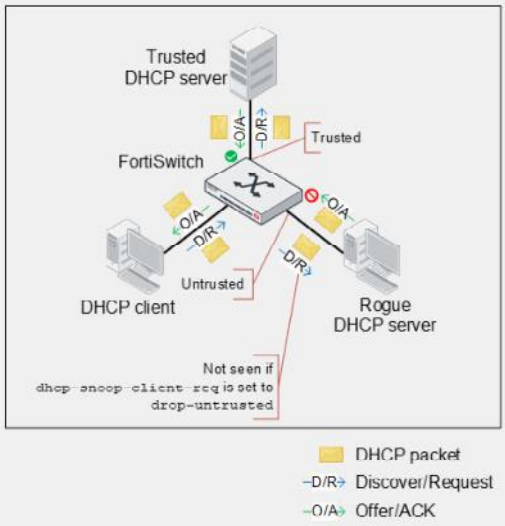
This slide also shows how to override the global settings on a specific port. Ports on managed switches are assigned a default storm control policy. The policy is configured to apply global settings on the port. If you want to override the settings, you can create another storm control profile, and assign it to the port as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

DHCP Snooping

- Inspects DHCP traffic to protect the network from:
  - Rogue DHCP servers
    - OFFER and ACK packets are accepted on trusted ports only
  - DHCP information leak
    - `dhcp-snoop-client-req` = `drop-untrusted`
    - DISCOVER and REQUEST packets are forwarded to trusted ports only
- Per-VLAN setting
  - Then, configure ports as trusted or untrusted



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

Any device in a network can potentially act as a DHCP server. A DHCP service can be enabled on a device by mistake, or on purpose by an attacker. For this reason, it's possible for DHCP clients to get their IP configuration from the wrong—untrusted—server. In addition, because DHCP requests are usually broadcasts, all devices in a broadcast domain receives a copy of the request, which results in a DHCP information leak.

DHCP snooping protects the DHCP service in your network from rogue DHCP servers and information leak by inspecting DHCP traffic and ensuring that:

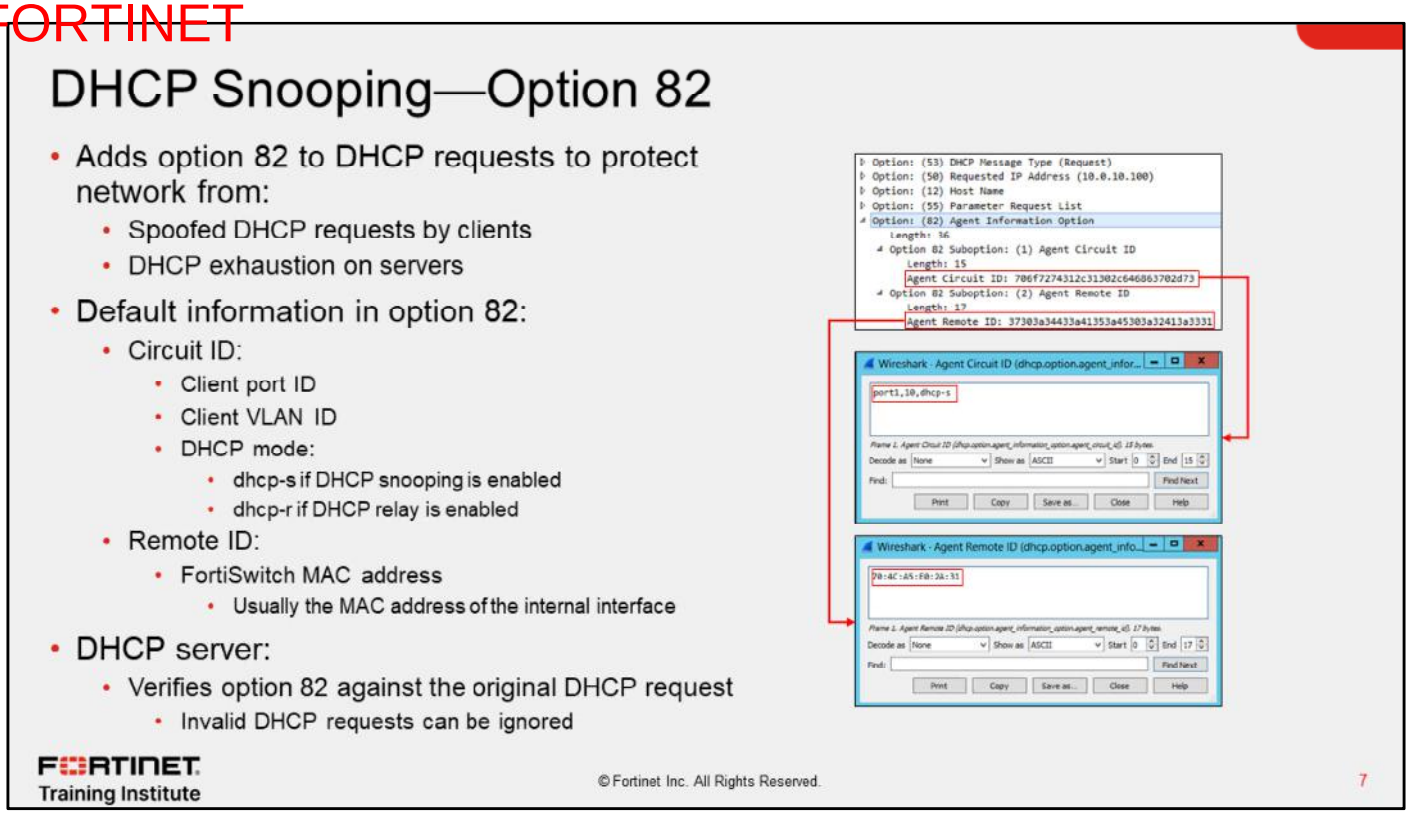
1. DHCP replies—OFFER AND ACK packets—are accepted on trusted ports only.
2. DHCP requests—DISCOVER and REQUEST packets—are forwarded to trusted ports only. This requires the FortiSwitchOS CLI `dhcp-snoop-client-req` setting to be set to `drop-untrusted`. By default, `dhcp-snoop-client-req` is set to `forward-untrust`, which means that DHCP requests are forwarded to untrusted ports.

You enable DHCP snooping on a VLAN, and then you configure a port as trusted or untrusted.

The example on this slide shows a switch with three endpoints connected. The port that connects the trusted DHCP server is configured as trusted, and the port that connects the rogue DHCP server as untrusted. The result is that FortiSwitch accepts DHCP replies from the trusted DHCP server only. DHCP replies sent by the rogue DHCP server are dropped by FortiSwitch. In addition, if `dhcp-snoop-client-req` is set to `drop-untrusted`, FortiSwitch forwards requests sent by the DHCP client to the trusted DHCP server only. In the example shown on this slide, this would result in the rogue DHCP server not receiving the DHCP request packet from the DHCP client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In addition to snooping DHCP traffic and dropping replies on untrusted ports, FortiSwitch can also insert option 82 to DHCP requests made on a VLAN.

Option 82, also known as DHCP relay agent information, can be used to protect the network against spoofing attacks on DHCP requests. When enabled, FortiSwitch adds option 82 to DHCP requests made by clients. Option 82 contains the following client-specific connection information by default:

- Circuit ID: Contains the client port ID, the client VLAN ID, and DHCP mode. The DHCP mode is dhcp-s when DHCP snooping is enabled, and dhcp-r when DHCP relay is enabled.
- Remote ID: Contains the FortiSwitch MAC address. This is usually the MAC address of the internal interface.

After FortiSwitch adds option 82 to the client DHCP request, it forwards the packet to trusted ports only. When FortiSwitch receives the reply from the server, FortiSwitch checks option 82 to identify the original request, removes option 82 from the packet, and then forwards the packet to the port that connects the client. Spoofing attacks on DHCP requests are prevented because a server can compare the information in option 82 against the information on the original DHCP request, and then decide whether the request is valid or not. Using option 82 can also protect the server against DHCP exhaustion attacks because servers avoid assigning IP addresses to spoofed requests.

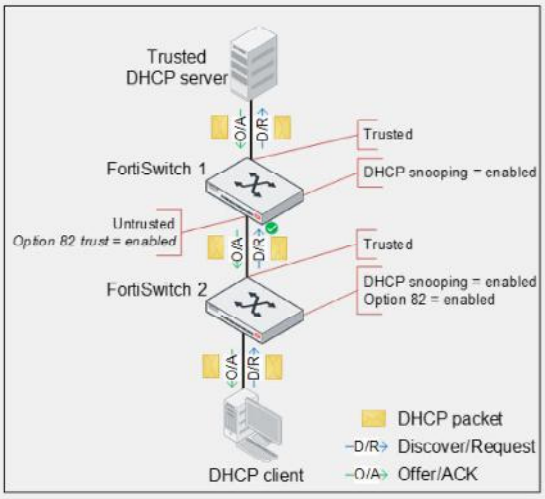
The image on this slide shows a packet capture displaying the circuit ID and remote ID suboptions in a DHCP REQUEST packet and their content in text format after being converted from ASCII by Wireshark. The information indicates that the client is connected to port1, assigned to VLAN 10, and that DHCP snooping is enabled. In addition, the MAC address of the FortiSwitch that inserted the option 82 information is `70:4C:A5:E0:2A:31`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

DHCP Snooping—Trusting Option 82 Added by Other Switches

- Trust DHCP requests with option 82 inserted by downstream switches
- Useful when switches are interconnected, and:
  - Upstream switch has DHCP snooping enabled
  - Ingress port on the upstream switch is untrusted
  - Upstream switch doesn't know option 82
    - Downstream switch inserts option 82



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

Usually, you want to enable DHCP snooping on all switches in your stack, but enable option 82 only on access switches, which is where DHCP clients are connected.

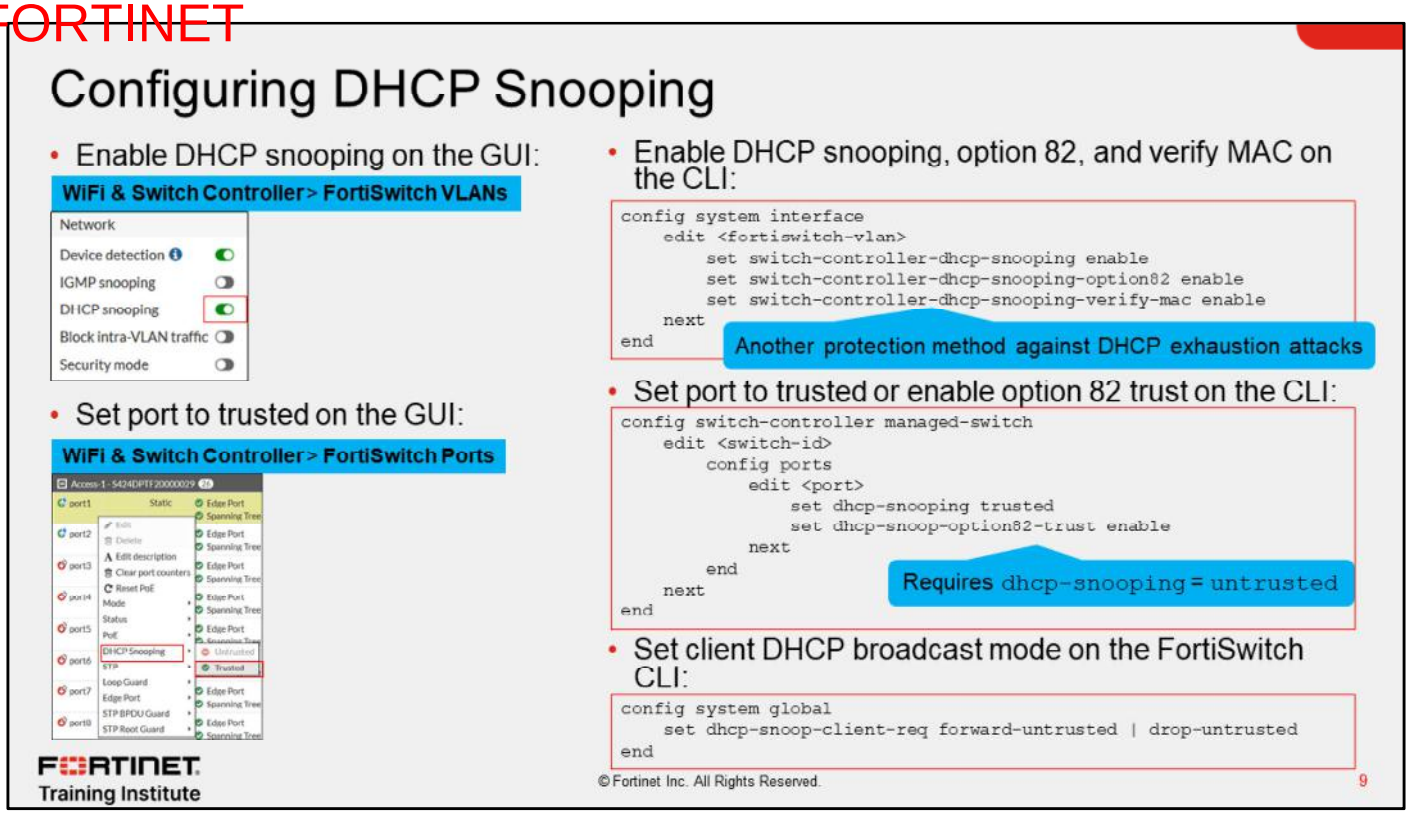
When DHCP snooping is enabled, DHCP requests with option 82 are dropped on untrusted ports. Because ports connecting downstream switches may be configured as untrusted—because there are no DHCP servers behind those ports—you must ensure that upstream switches accept, on ISL ports, DHCP requests with option 82 that were inserted by downstream switches.

The topology on this slide illustrates the example described. There are two switches interconnected. Both switches have DHCP snooping enabled, but only FortiSwitch 2 has option 82 enabled. Also, FortiSwitch 1 connects to the trusted DHCP server and FortiSwitch 2 to the DHCP client. Because the port on FortiSwitch 1 that connects to FortiSwitch 2 is configured as untrusted, you must ensure the port *trusts* incoming DHCP messages with option 82 that were forwarded by FortiSwitch 2. Otherwise, FortiSwitch 1 drops the packet during option 82 verification because it doesn't recognize the information in it.

In the example shown on this slide, the port is configured to trust incoming DHCP packets with option 82. For this reason, DHCP requests forwarded by FortiSwitch 1 are accepted by the port and forwarded to the trusted DHCP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



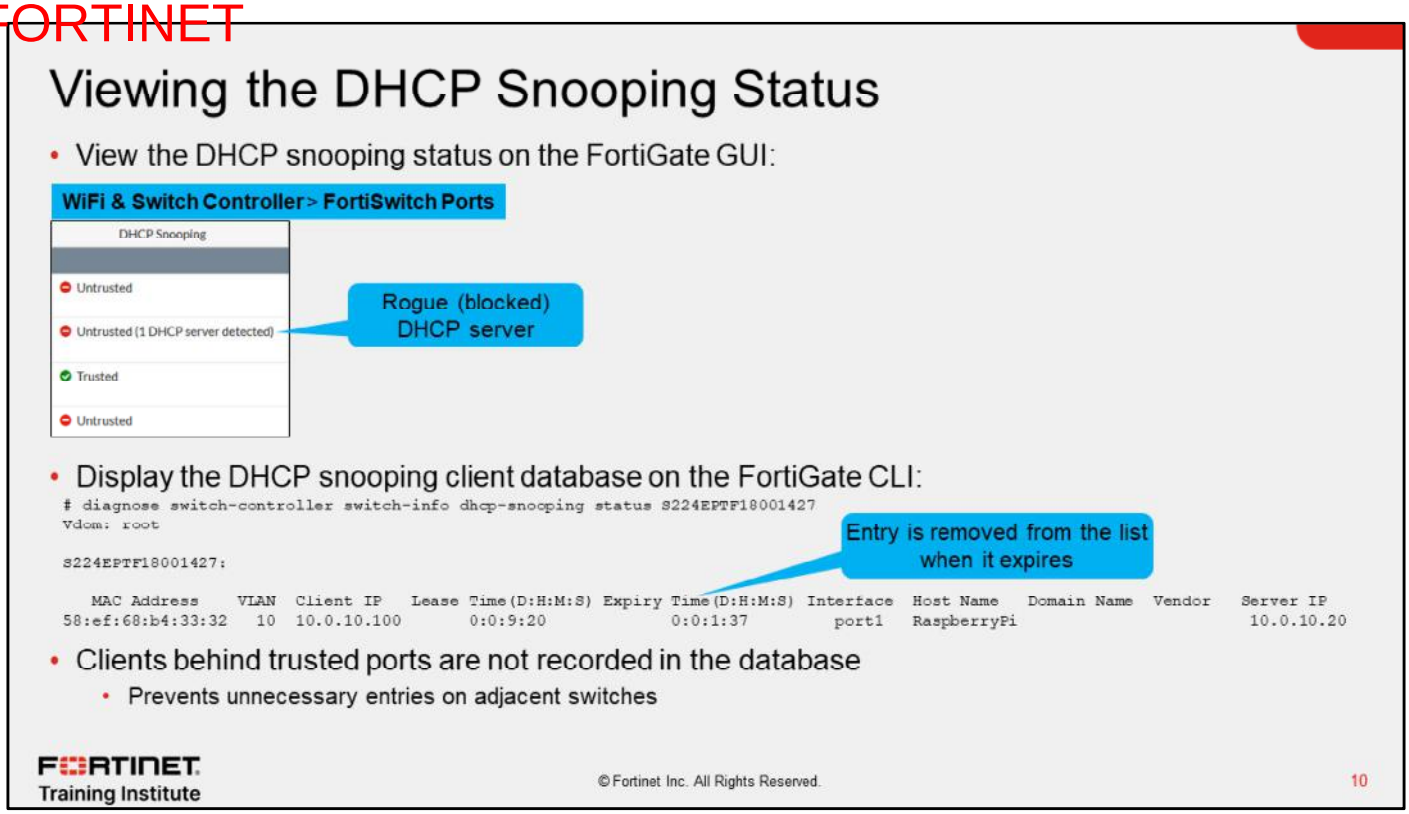
DHCP snooping is disabled by default. This slide shows how to use the FortiGate GUI to enable DHCP snooping on a VLAN and how to configure a port as trusted. The equivalent settings on the FortiGate CLI are also shown. Note that the settings related to option 82 and verify MAC are available on the FortiGate CLI only.

The verify MAC setting (`switch-controller-dhcp-snooping-verify-mac`) instructs FortiSwitch to verify that the source MAC address in the Ethernet header and the client hardware address in the DHCP header match in the DHCP packets that are received on untrusted ports. When FortiSwitch verifies the MAC address on the DHCP packets, it prevents exhaustion on your DHCP server and on the switch DHCP snooping client database. When the DHCP snooping client database reaches its limit, FortiSwitch doesn't add more clients to the database, and as a result, drops the DHCP requests from the affected clients. FortiSwitch also generates logs to inform the user that the DHCP client database is full. DHCP traffic from other clients with an existing entry in the database is not affected.

In addition, `dhcp-snoop-option82-trust` is meant to be enabled on a port only when the port is configured as untrusted. The goal is to allow only DHCP packets with option 82 on untrusted ports, while dropping DHCP replies without option 82. If you configure a port as trusted, all DHCP replies are accepted regardless of whether the packets contain option 82. You may need to enable `dhcp-snoop-option82-trust` on a port where the trusted DHCP server and other untrusted devices are connected. In this case, it's better to enable option 82 on FortiSwitch, and then have the switch restrict DHCP replies to those containing option 82. This enables you to accept legitimate replies from the trusted DHCP server while dropping potential spoofed replies made by other devices in the shared segment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **DHCP Snooping** column on the FortiGate **FortiSwitch Ports** page shows whether ports have been configured as **Trusted** or **Untrusted**. The page also indicates when a rogue DHCP server has been detected behind an untrusted port, meaning that the replies from the DHCP server are being blocked by FortiSwitch.

On the FortiGate CLI, you can use the command shown on this slide to get a list of DHCP clients detected by a managed switch using DHCP snooping. For each client, DHCP-related information, such as MAC address, VLAN, client and server IP, is included. Note that FortiSwitch keeps track of the DHCP lease time for each entry. If the client doesn't renew the lease before it expires, FortiSwitch removes the entry from the list.

Also note that FortiSwitch records DHCP clients that are connected to untrusted ports only. This prevents unnecessary entries in the client database of adjacent switches that also perform DHCP snooping.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing the DHCP Snooping Status (Contd)

- View the DHCP snooping database on the FortiGate CLI:

```
# diagnose switch-controller switch-info dhcp-snooping database S224EPTF18001427
Vdom: root

S224EPTF18001427:

snoop-enabled-vlans             : 10
verifysrcmac-enabled-vlans      :
option82-enabled-vlans          : 10
option82-trust-enabled-intfs    :
trusted ports     : port2 _FlInK1_MLAG0_
untrusted ports   : port1 port3 port4 port5 port6 port7 port8 port9 port10 port11
                    port12 port13 port14 port15 port16 port17 port18 port19 port20 port21
                    port22 port25 port26 port27 port28
Max Client Database Entries       : 2000
        Client Database           : 1
        Client6 Database          : 0
Max Server Database Entries       : 256
        Server Database           : 1
        Server6 Database          : 0
Limit Database           : 1 / 256

DHCP Global Configuration:
==========================
DHCP Broadcast Mode               : All
DHCP Allowed Server List          : Disable
Add hostname in Option82          : Disable
```

Max. entries is model-specific

forward-untrusted

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

The FortiOS CLI command shown on this slide displays a summary of the DHCP snooping configuration on a managed switch. The output indicates the interfaces that are set as trusted and untrusted, the VLANs where DHCP snooping is enabled on, as well as the maximum and current number of entries in the database. The maximum number of entries varies among models. Higher-end FortiSwitch models support a higher number of database entries. When the DHCP snooping client database reaches its limit, FortiSwitch doesn't add more clients to the database, and drops the DHCP requests from those clients.

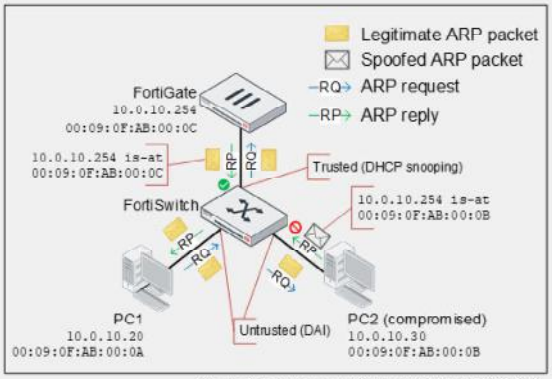
The output also includes the global configuration for DHCP snooping. In the example shown on this slide, the `DHCP Broadcast Mode` is set to `All` (`forward-untrusted`).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Dynamic ARP Inspection (DAI)

- Prevents ARP spoofing and MITM attacks
- Works as follows:
  - Checks ARP packets against:
    - DHCP snooping client DB (DHCP clients)
    - IPSG DB (static IP clients)
  - Drops ARP packets on untrusted ports without valid IP-MAC binding in DB
    - Checks MAC, IP, interface, and VLAN
  - Allows ARP packets on trusted ports (DHCP snooping or DAI)
    - Inspection is skipped
- Per-VLAN setting
  - Ports are then configured as trusted or untrusted



Note: No entries configured in the IPSG DB

DHCP Snooping Client DB			
MAC	VLAN	IP	Interface
00:09:0F:AB:00:0A	10	10.0.10.20	port1
00:09:0F:AB:00:0B	10	10.0.10.30	port2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

ARP spoofing, also known as ARP poisoning, is another attack that can be easily performed within a broadcast domain. An attacker can flood the network with forged ARP replies to poison the ARP table of other devices. The goal is to perform a man-in-the-middle (MITM) attack by tricking a victim to redirect its network traffic to a compromised device. The victim believes that it is communicating directly with its intended target, when in fact it's doing so indirectly through another device unknowingly.

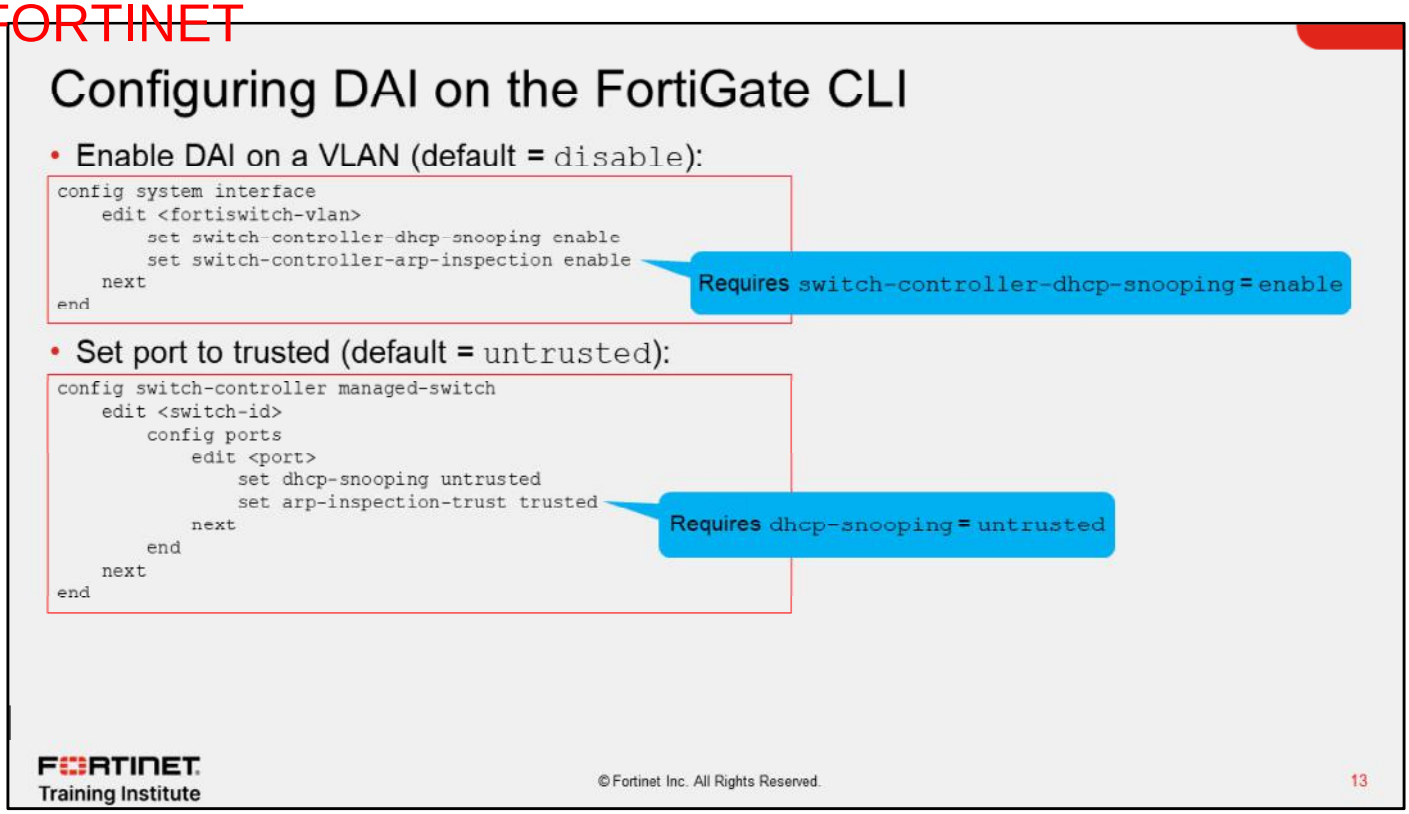
DAI prevents ARP spoofing by checking that ARP packets on untrusted ports have a valid IP-MAC address binding entry in the DHCP snooping client database or in the IP source guard (IPSG) database. When checking for a valid entry in the database, DAI considers the MAC address, IP address, interface, and VLAN involved. DAI relies on DHCP snooping to verify ARP packets from DHCP clients, and on IPSG for static IP clients. You will learn more about IPSG in this lesson.

You enable DAI on a VLAN, and then configure a port as trusted or untrusted for DAI. DAI performs ARP inspection on ports that have been configured as untrusted for DAI, and skips inspection on ports that have been configured as trusted in either DHCP snooping or DAI. DAI implicitly trusts ports configured as trusted in DHCP snooping.

The topology on this slide shows three endpoints connected to FortiSwitch. All endpoints are placed in VLAN 10. FortiGate acts as the DHCP server and is connected to a trunk, which is configured as trusted for DHCP snooping. The two PCs are connected to ports configured as untrusted for DAI. There are no entries configured in the IPSG database. PC2 is compromised and trying to spoof FortiGate by sending forged ARP replies that advertise the FortiGate IP address as bound to its local MAC address. However, because DAI is enabled on the VLAN and ARP replies sent by PC2 don't have a matching IP-MAC address binding in the DHCP snooping client database or IPSG database, the packets fail ARP inspection and are dropped by FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

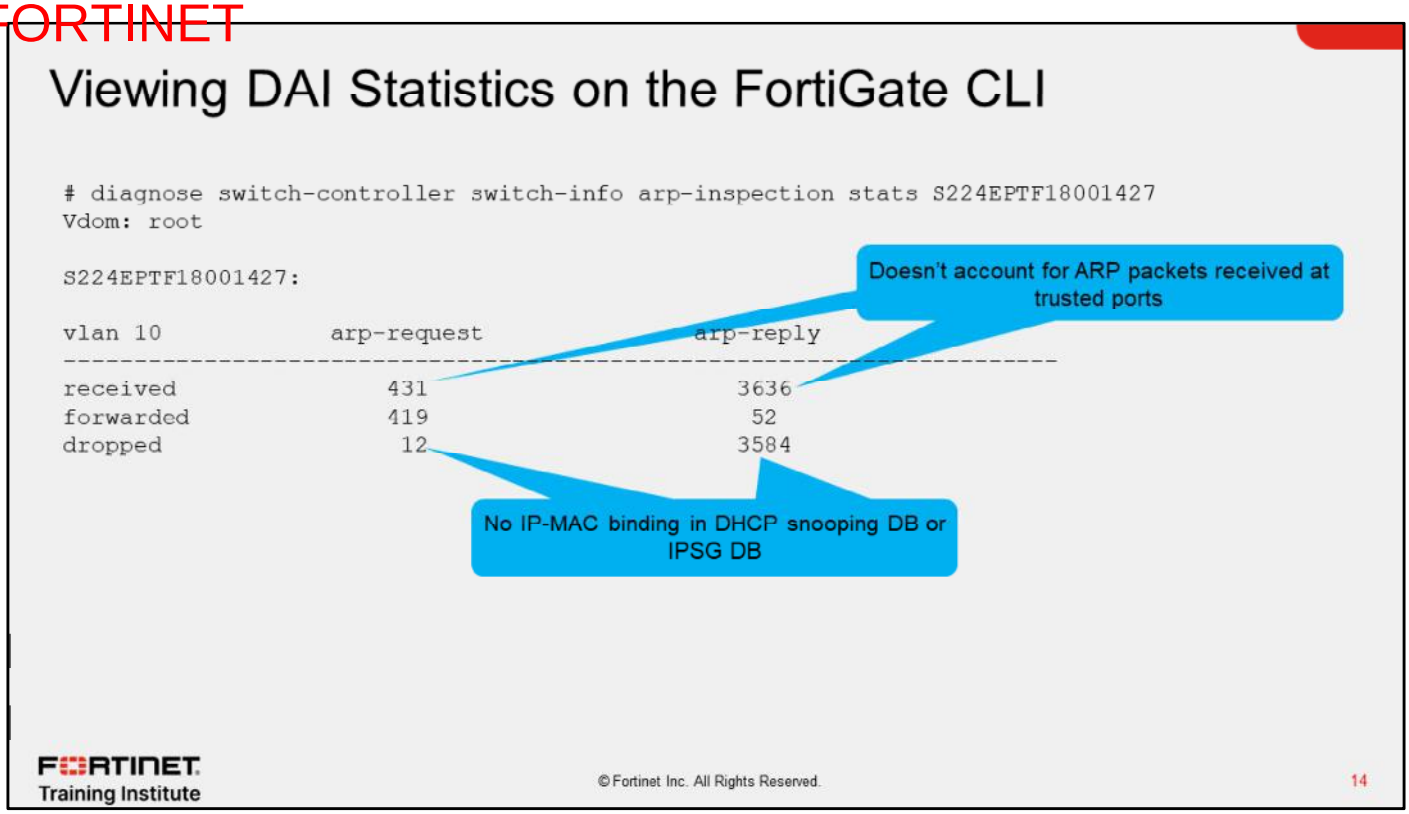


DAI is disabled by default. You must use the FortiGate CLI to enable DAI on a VLAN and to configure a port as trusted, as shown on this slide.

You can enable DAI on a VLAN only if you previously enabled DHCP snooping on that VLAN. Also, all ports are set as untrusted in DAI by default. However, note that a port is implicitly trusted in DAI when it is trusted in DHCP snooping, which is why `arp-inspection-trust` is available only when `dhcp-snooping` is set to `untrusted`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiOS CLI command shown on this slide displays DAI statistics on a managed switch. The output shows how many ARP request and reply packets have been received (inspected), and how many packets were forwarded or dropped. If there is a valid IP-MAC binding in the DHCP snooping client database or in the IPSG database, the packet is forwarded. Otherwise, the packet is dropped.

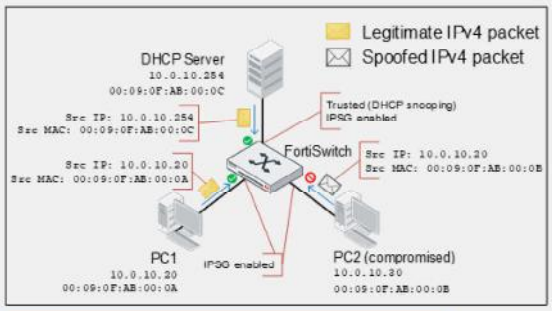
Note that the `received` counter shown in the output, increments only when ARP packets are received at untrusted ports. FortiSwitch does not inspect ARP packets received on trusted ports, and therefore, these packets are not included in the DAI statistics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP Source Guard (IPSG)

- Prevents IP spoofing attacks
- Works as follows:
  - Allows DHCP traffic always
  - Checks IPv4 packets (except DHCP) against:
    - IPSG DB
      - Dynamic entries imported from DHCP snooping client DB
      - Static entries added by the administrator
  - Drops IPv4 packets without matching IP-MAC binding in IPSG DB
    - Checks source MAC, source IP, and interface
- Per-port setting



DHCP Snooping Client DB

MAC	VLAN	IP	Interface
00:09:0F:AB:00:0A	10	10.0.10.20	port1
00:09:0F:AB:00:0B	10	10.0.10.30	port2

IPSG DB

MAC	IP	Interface	Type
00:09:0F:AB:00:0A	10.0.10.20	port1	Dynamic
00:09:0F:AB:00:0B	10.0.10.30	port2	Dynamic
00:09:0F:AB:00:0C	10.0.10.254	port3	Static

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

An IP spoofing attack is performed by sending IP packets with forged source IP addresses. The goal is for an attacker to hide their real identity or to impersonate another device in the network, or both.

IPSG prevents spoofing on IPv4 traffic by verifying that there is an IP-MAC binding in the IPSG database that matches the source IP and source MAC addresses of the packet.

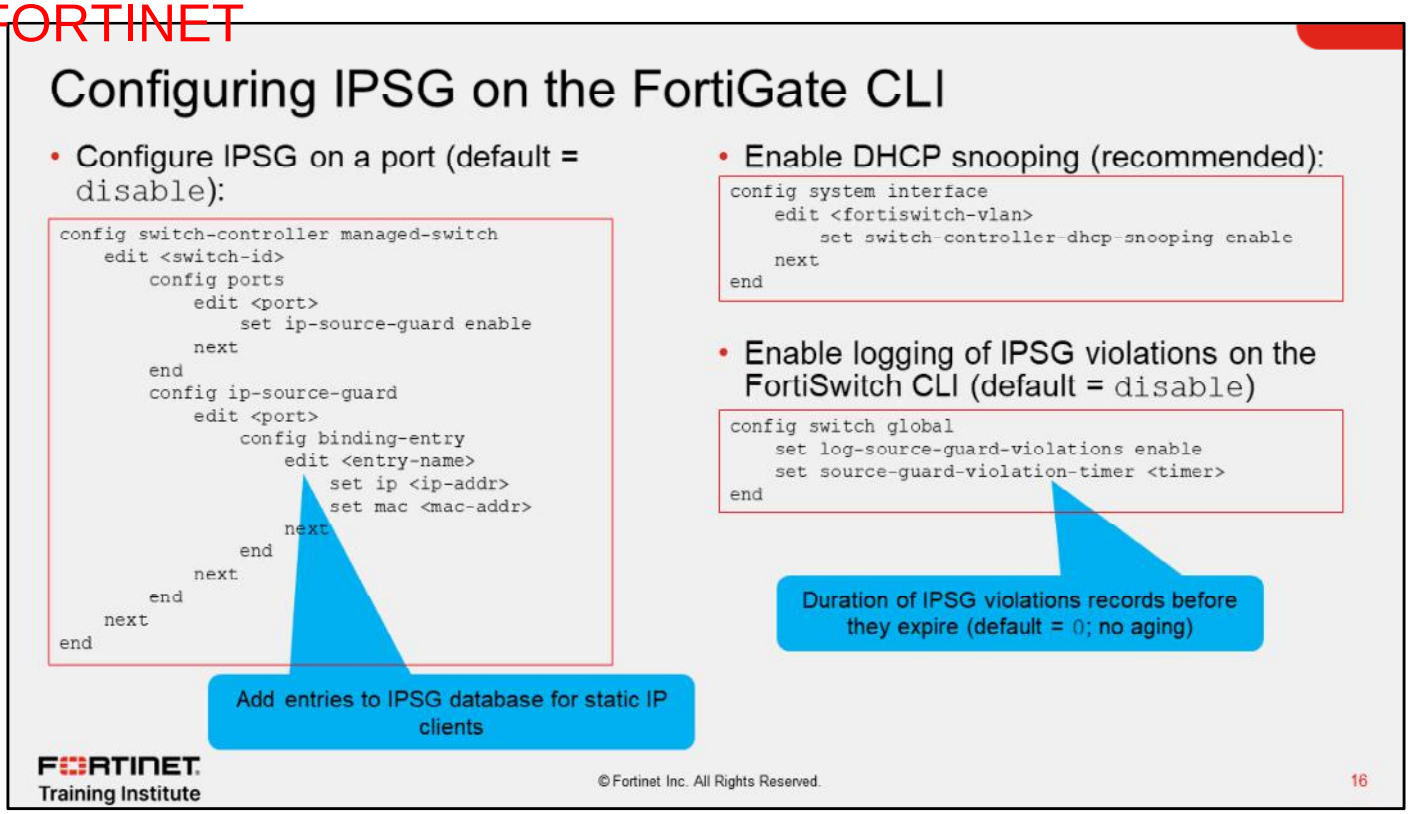
You enable IPSG on a port. FortiSwitch then allows DHCP traffic on the port so the endpoint can obtain an IP address through DHCP. When the endpoint generates IPv4 traffic other than DHCP traffic, FortiSwitch compares the source IP and source MAC addresses of the packet against the entries in the IPSG database. If there is a match, the packet is allowed; otherwise, it's dropped.

The IPSG database is composed of dynamic and static entries. Dynamic entries are imported from the DHCP snooping client database. Static entries are manually configured by the administrator.

The topology on this slide shows a DHCP server and two PCs. The PCs obtain their IP configuration from the DHCP server. IPSG is enabled on all switch ports. Because DHCP snooping is also enabled, the IPSG database imports the information for dynamic entries from the DHCP snooping client database. The DHCP server uses a static IP address, so the administrator configured an entry for the device in the IPSG DB. The result is that FortiSwitch allows IPv4 packets sent by PC1 and the DHCP server because the source MAC and source IP addresses in the packet have a matching IP-MAC binding entry in the IPSG database. However, FortiSwitch blocks spoofed IPv4 packets sent by PC2 because there isn't a matching entry in the IPSG database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



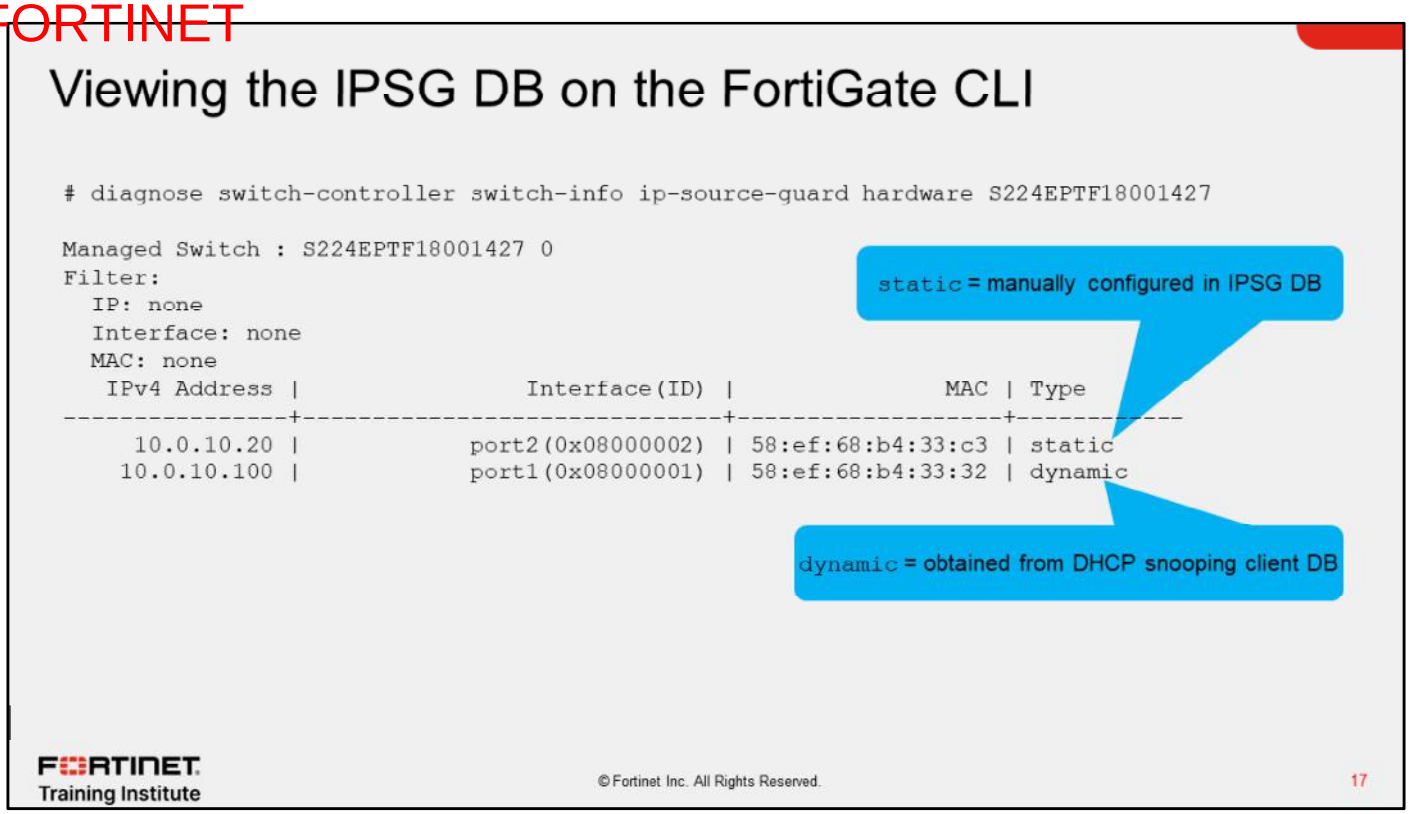
IPSG is disabled by default. You must use the FortiGate CLI to enable IPSG on a per-port basis, and to manually configure IP-MAC binding entries in the IPSG database for endpoints using static IP addresses.

DHCP snooping is not required for IPSG to work, but it is recommended. Otherwise, you would have to manually configure an entry in the IPSG database for each connected endpoint. When you enable DHCP snooping, entries for DHCP clients—dynamic entries—are automatically imported from the DHCP snooping client database, which reduces the administrative overhead considerably.

By default, IPSG doesn't generate any logs when it drops packets. If you want to log IPSG violations, you must enable the corresponding setting on the FortiSwitch CLI as shown on this slide. After you enable the logging of IPSG violations, you can also set a timer for these events. By default, the timer is set to `0`, which means that the violation events won't expire.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

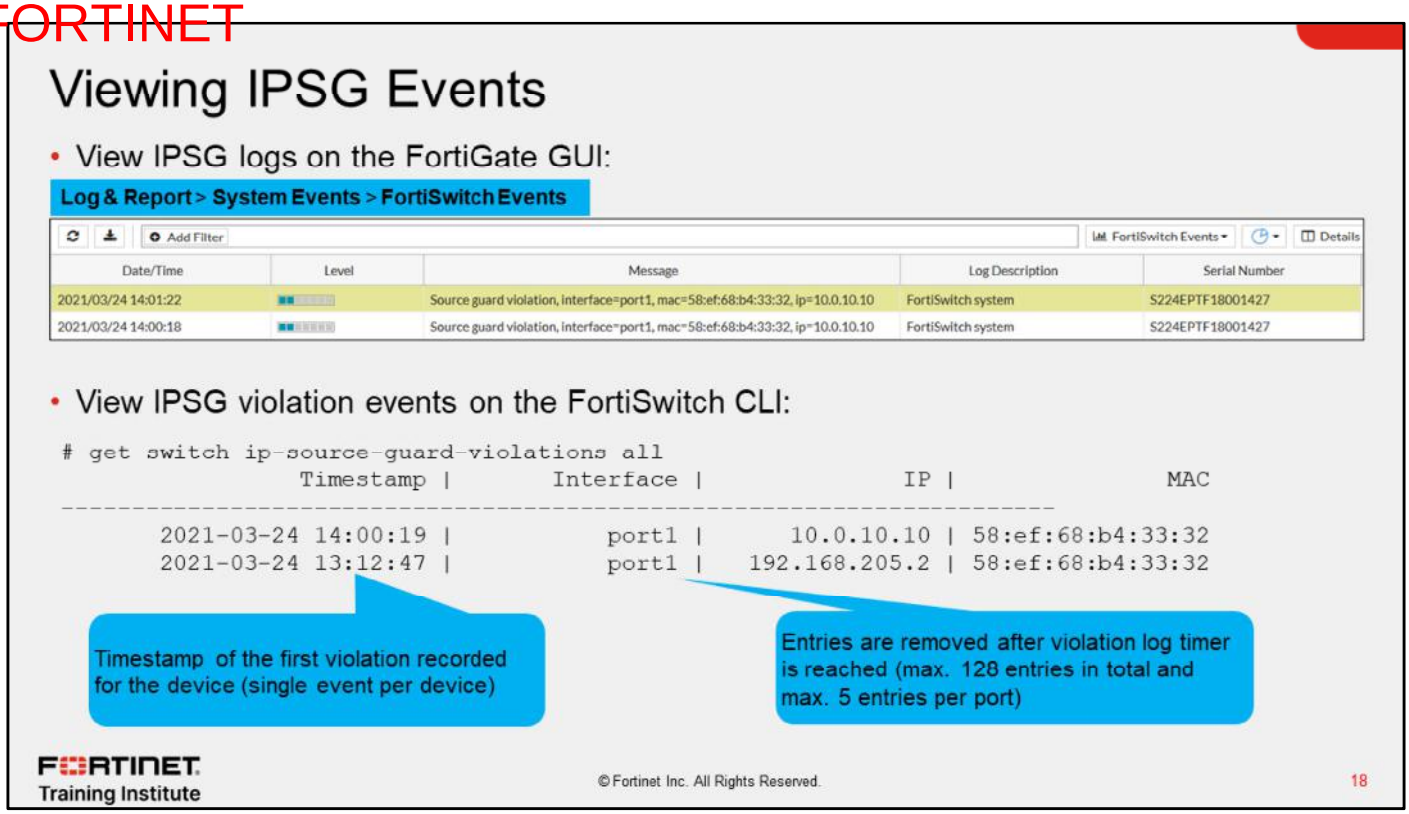


The FortiOS CLI command shown on this slide displays the IPSG database on a managed switch. The output indicates whether the entry is static or dynamic. Static entries are manually configured by the administrator, while dynamic entries are automatically imported from the DHCP snooping client database.

Note that not all entries in the DHCP snooping client database are imported. Only entries for endpoints connected to ports with IPSG enabled are imported.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



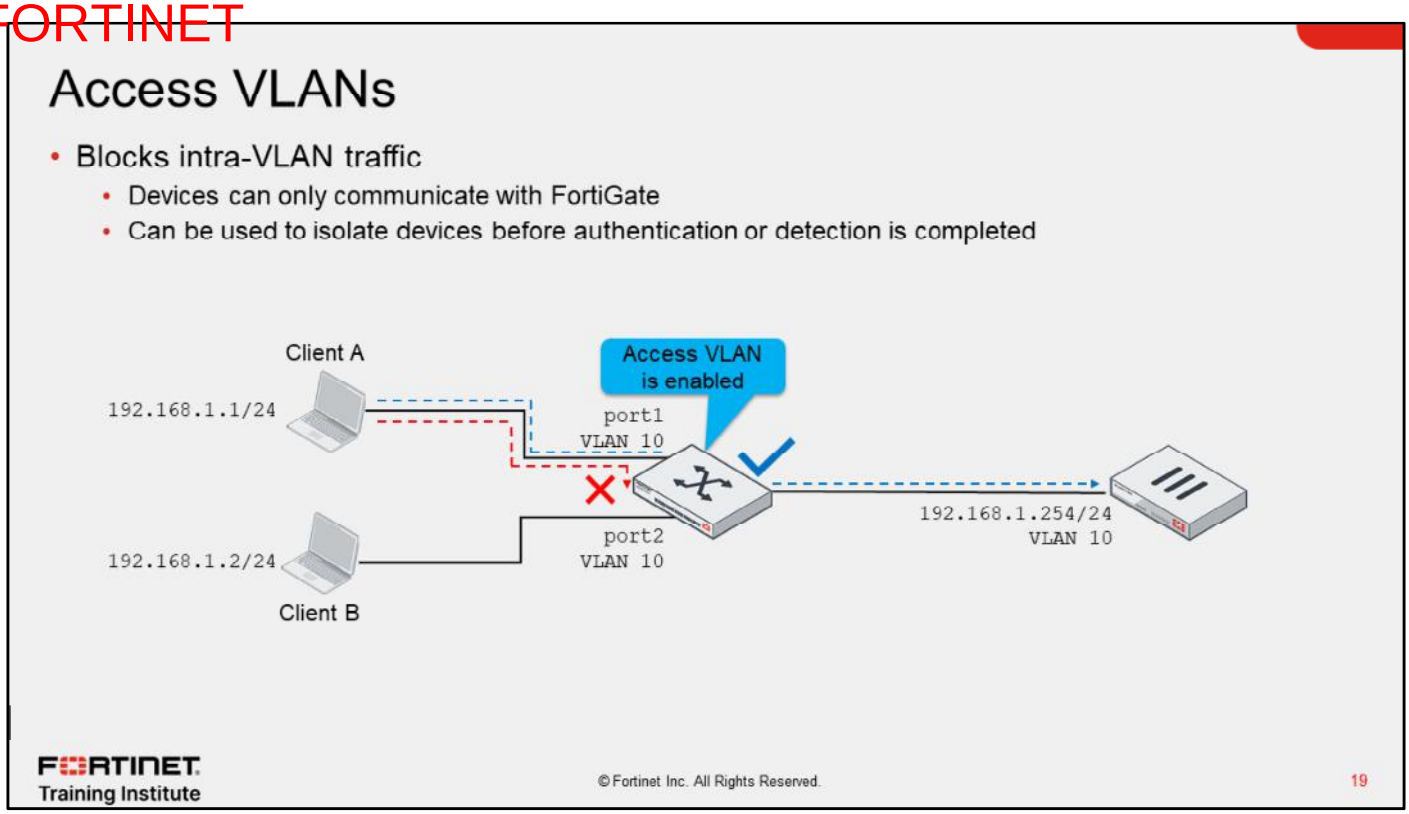
You can view IPSG violation logs on the FortiGate GUI by browsing to the **FortiSwitch Events** subcategory.

In addition to logs, FortiSwitch also keeps a list of IPSG violations. You can view this list on the FortiSwitch CLI only by running the command shown on this slide. If you set a violation log timer to a value other than zero, the entries in this list are removed after the timer is reached. The timestamp shown for each event corresponds to the time of the first recorded violation. The list shows a single event per device, even if FortiSwitch has blocked multiple packets from that device.

Note that the list supports up to 128 entries in total and up to 5 entries per port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



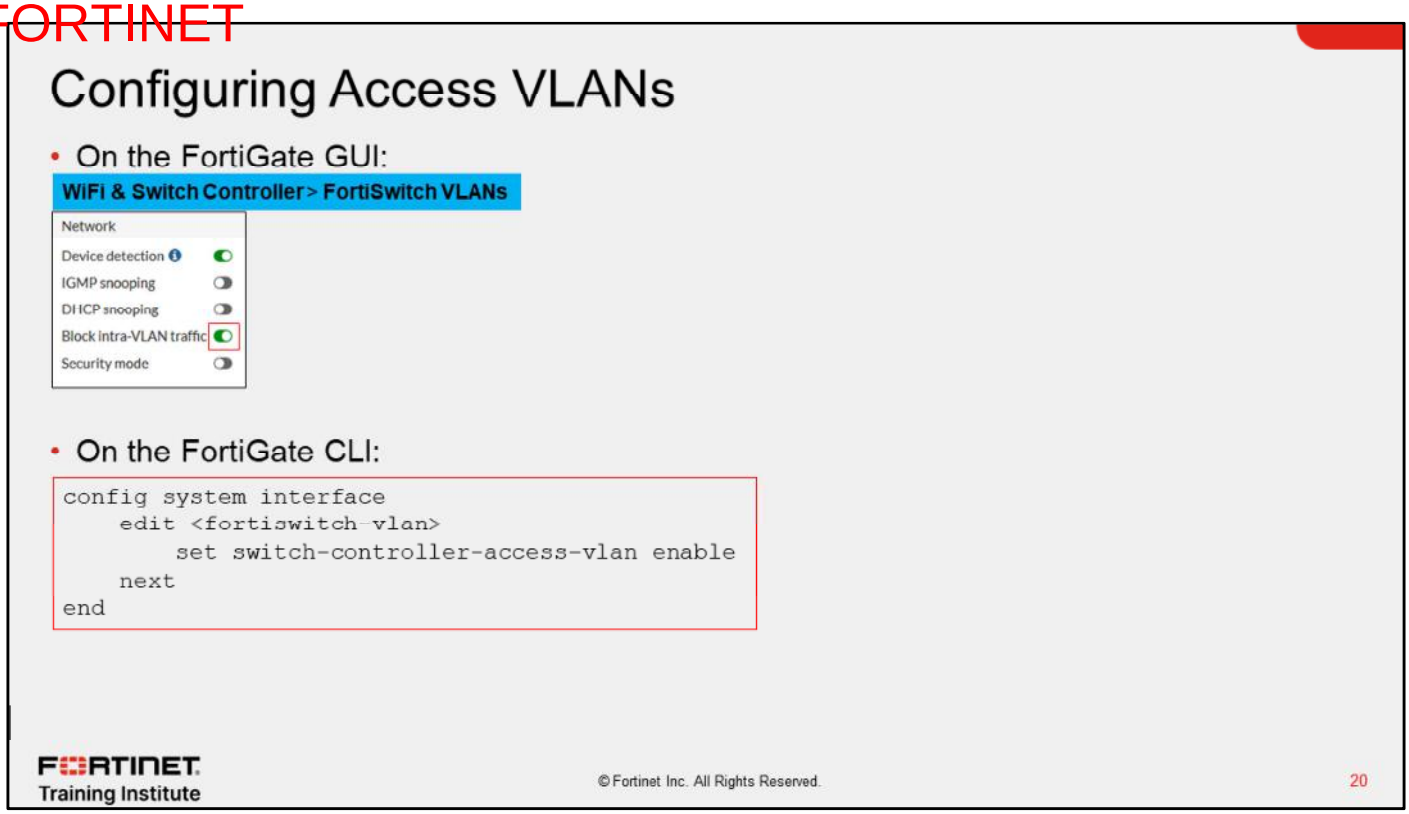
Access VLANs enable FortiSwitch to prevent direct communication among devices in the same VLAN. Devices can communicate with FortiGate only. Traffic destined to other devices in the same VLAN is dropped by FortiSwitch. Although other vendors use the term access VLAN when referring to the native or untagged VLAN on a switch port, in FortiSwitch, access VLAN refers to a VLAN that allows traffic to the switch controller only.

Access VLANs can be used to place devices in a temporary or onboarding VLAN before they are authenticated or identified by FortiGate, after which FortiGate moves the device to the corresponding production VLAN. Another use case for access VLANs is when you want to drop intra-VLAN traffic because the devices don't require client-to-client communication. This could prevent the spread of malware by compromised hosts, reduce the amount of traffic in the network, or prevent an attacker from gathering network information that can be used to attack vulnerable hosts in the same VLAN.

In the network diagram shown on this slide, port1 and port2 on FortiSwitch are placed in VLAN 10, which is a FortiSwitch VLAN on FortiGate with access VLAN enabled. As a result, when client A sends traffic destined to devices other than the VLAN 10 interface on FortiGate, the traffic is dropped by FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can enable access VLANs on the FortiGate GUI by enabling **Block intra-VLAN traffic** on the corresponding FortiSwitch VLAN. Alternatively, you can run the FortiOS CLI commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

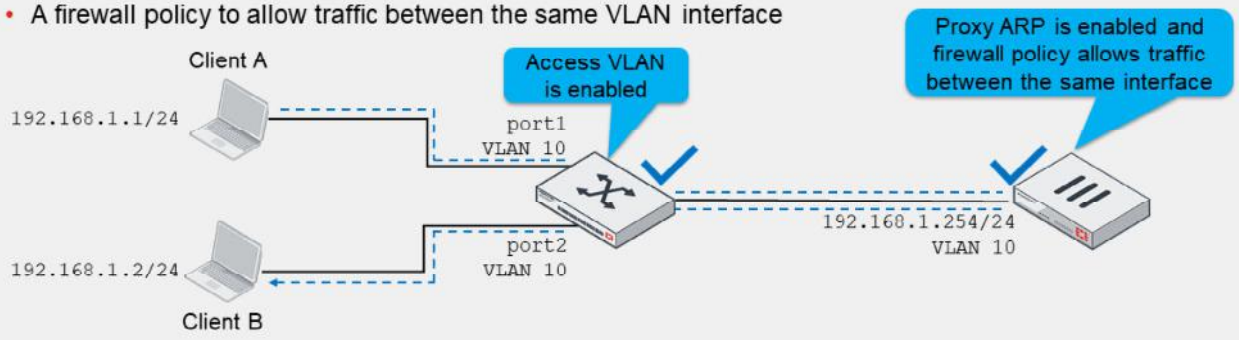
DO NOT REPRINT Brave-dumps.com
© FORTINET

Access VLANs—Allow Intra-VLAN Traffic

- Intra-VLAN communication *through* FortiGate can be allowed by configuring:
  - Proxy ARP on FortiGate, for example:

```
config system proxy-arp
    edit 1
        set interface "VLAN 10"
        set ip 192.168.1.1
        set end-ip 192.168.1.253
    next
end
```

  - A firewall policy to allow traffic between the same VLAN interface



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

When access VLAN is enabled, you can still allow intra-VLAN traffic *through* FortiGate by having FortiGate perform proxy ARP for other hosts in the VLAN, and by having firewall policies allowing the intra-VLAN traffic.

This slide shows an example of the proxy ARP configuration needed on FortiGate, based on the network diagram shown on the slide. When client A sends ARP requests for resolving the MAC address of client B, FortiGate responds to ARP requests on behalf of client B. As a result, when client A communicates with client B, packets from client A to client B are sent through FortiGate, which is traffic that is allowed by FortiSwitch. When traffic arrives at FortiGate, the traffic is then forwarded to client B because FortiGate has a firewall policy allowing the intra-VLAN traffic.

When you configure the firewall policy, you must select the same VLAN interface as the incoming interface and the outgoing interface. You can also enable security profiles to perform inspection, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about storm control is true?
   - ✓ A. The configured global threshold is enforced independently on each switch port.
   - B. Storm control is enabled by default.

2. What action does FortiSwitch take on DHCP replies received on ports configured as trusted for DHCP snooping?
   - A. FortiSwitch drops the DHCP replies.
   - ✓ B. FortiSwitch forwards the DHCP replies.

3. Which database is used by DAI to check valid IP-MAC bindings for static IP clients?
   - ✓ A. The IPSG database
   - B. The DHCP snooping client database

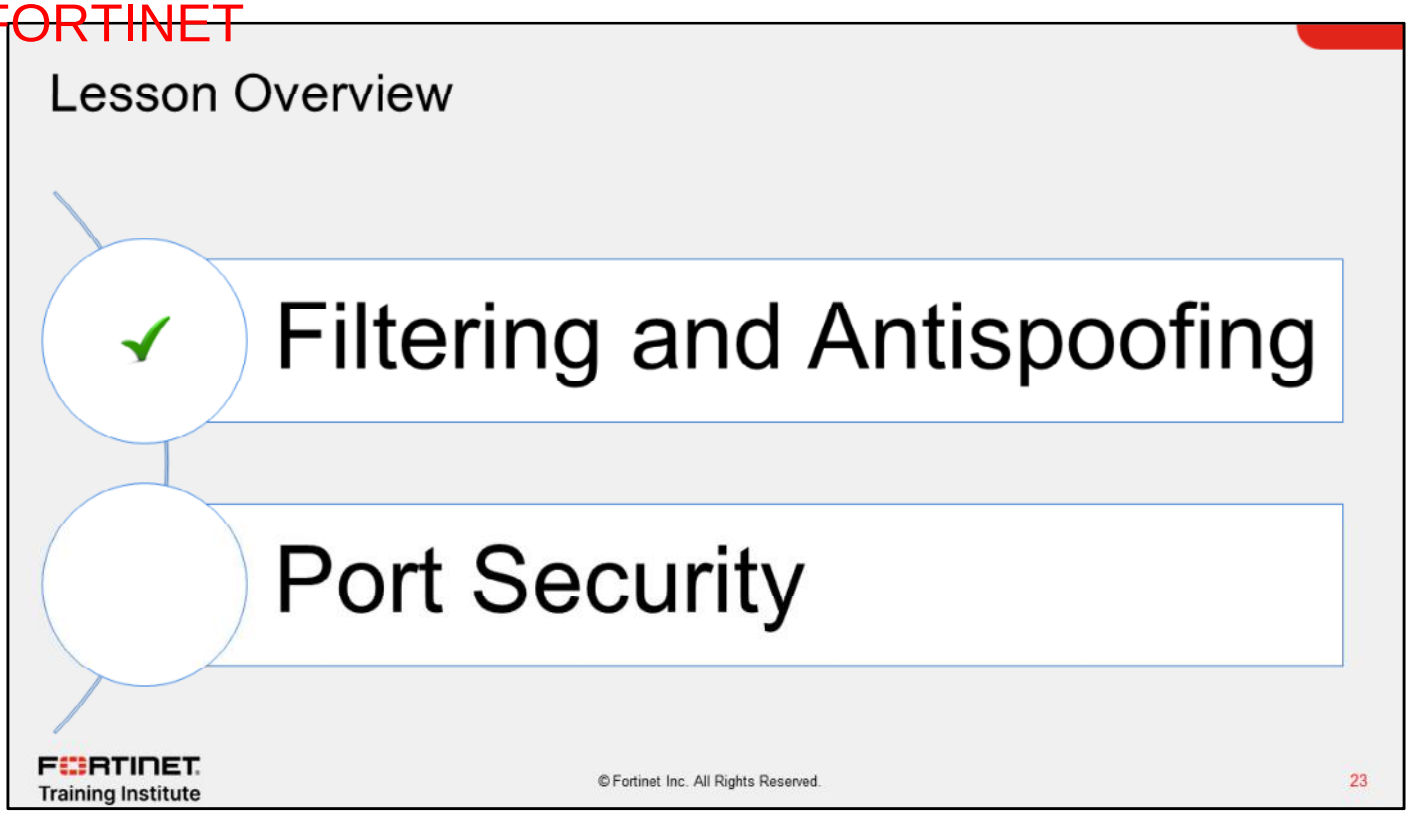
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

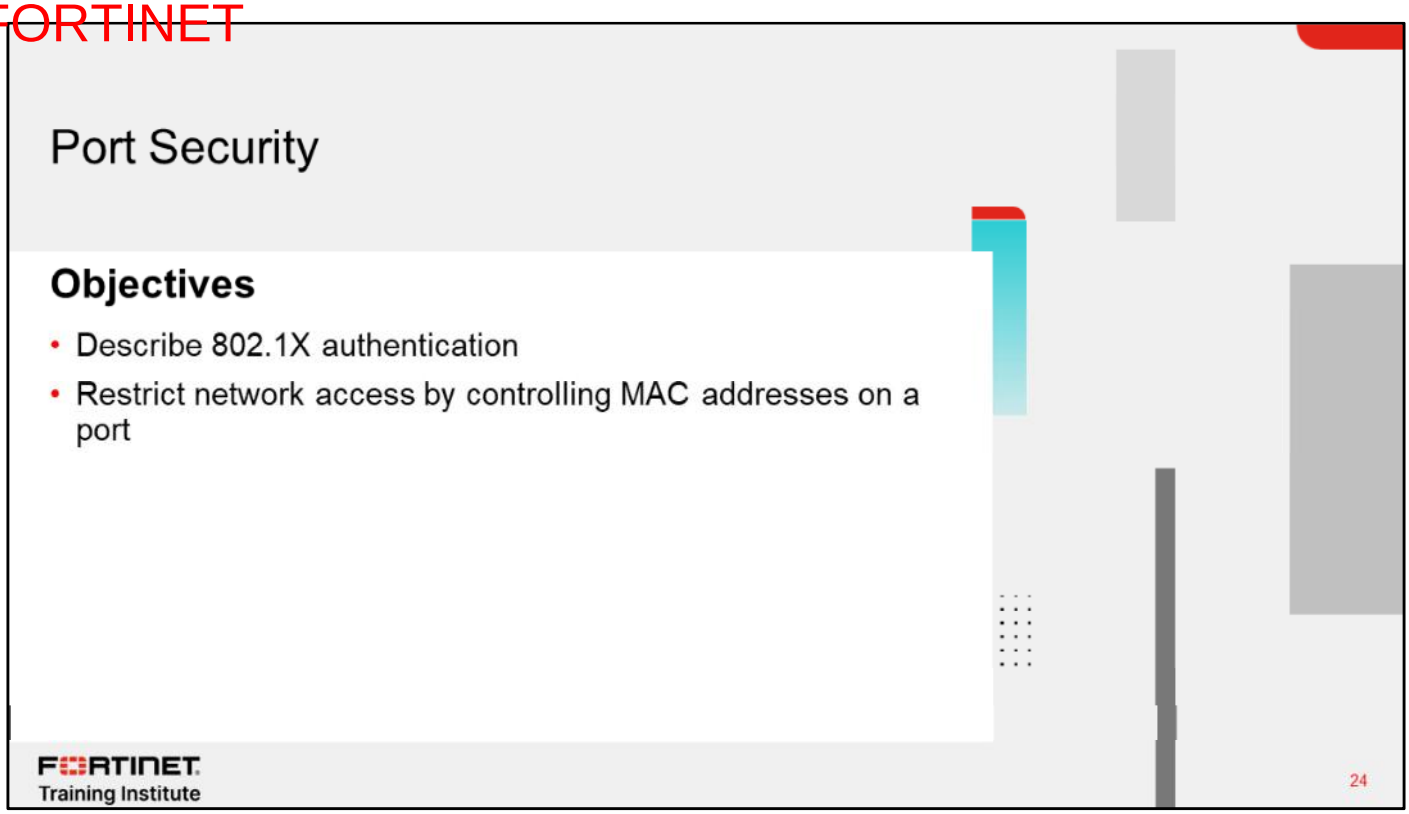


Good job! You now understand filtering and antispoofing.

Now, you will learn about port security.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

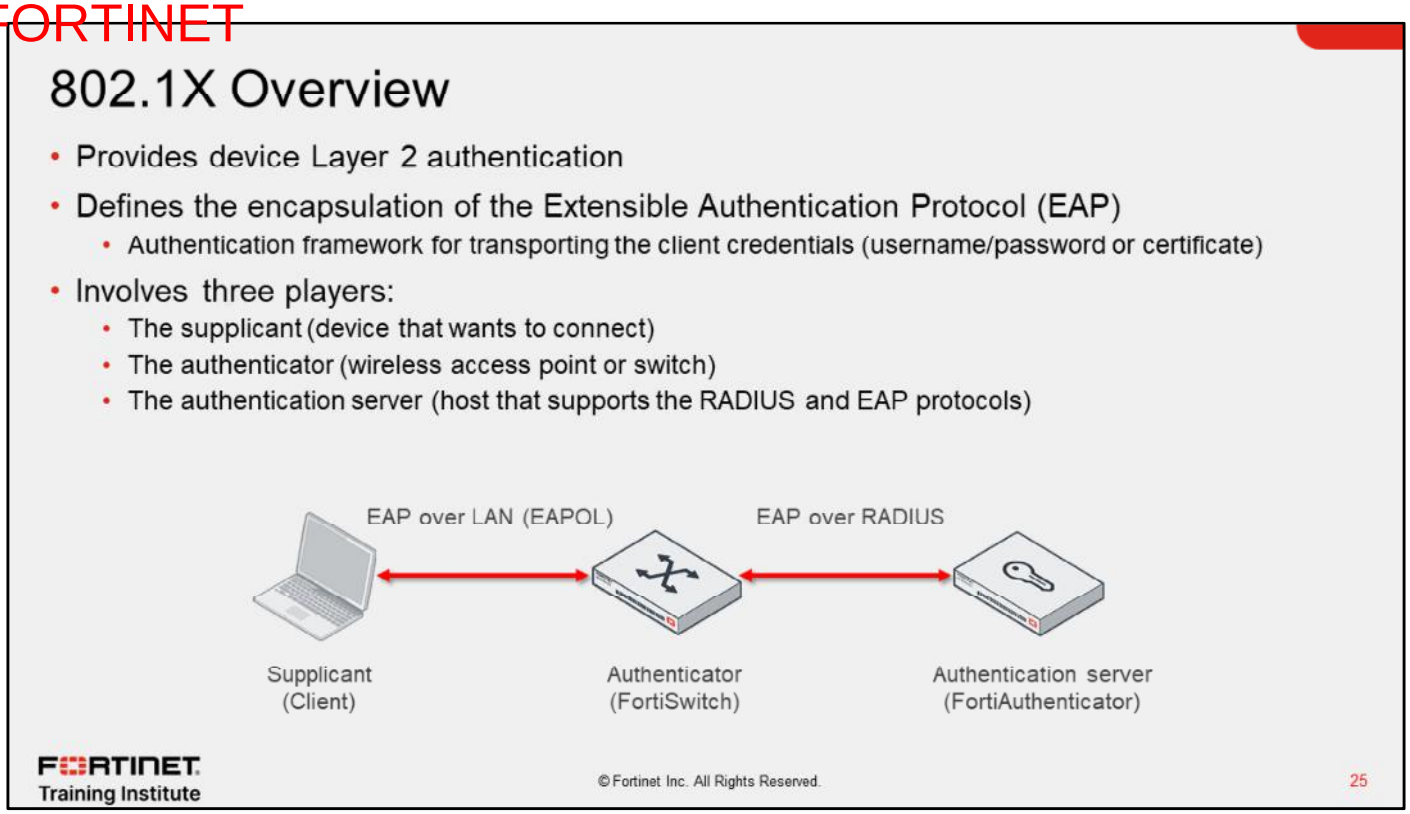


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in port security, you will understand how to provide secure access to network devices using 802.1X authentication and by restricting the MAC addresses allowed on a port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



802.1X is a standard that is designed to provide authentication services to network devices that want to join a wired or wireless network. The 802.1X standard defines an authentication protocol called EAP. It also defines how EAP is encapsulated over the LAN—the EAPOL protocol—and over RADIUS.

802.1X involves the following three parties:

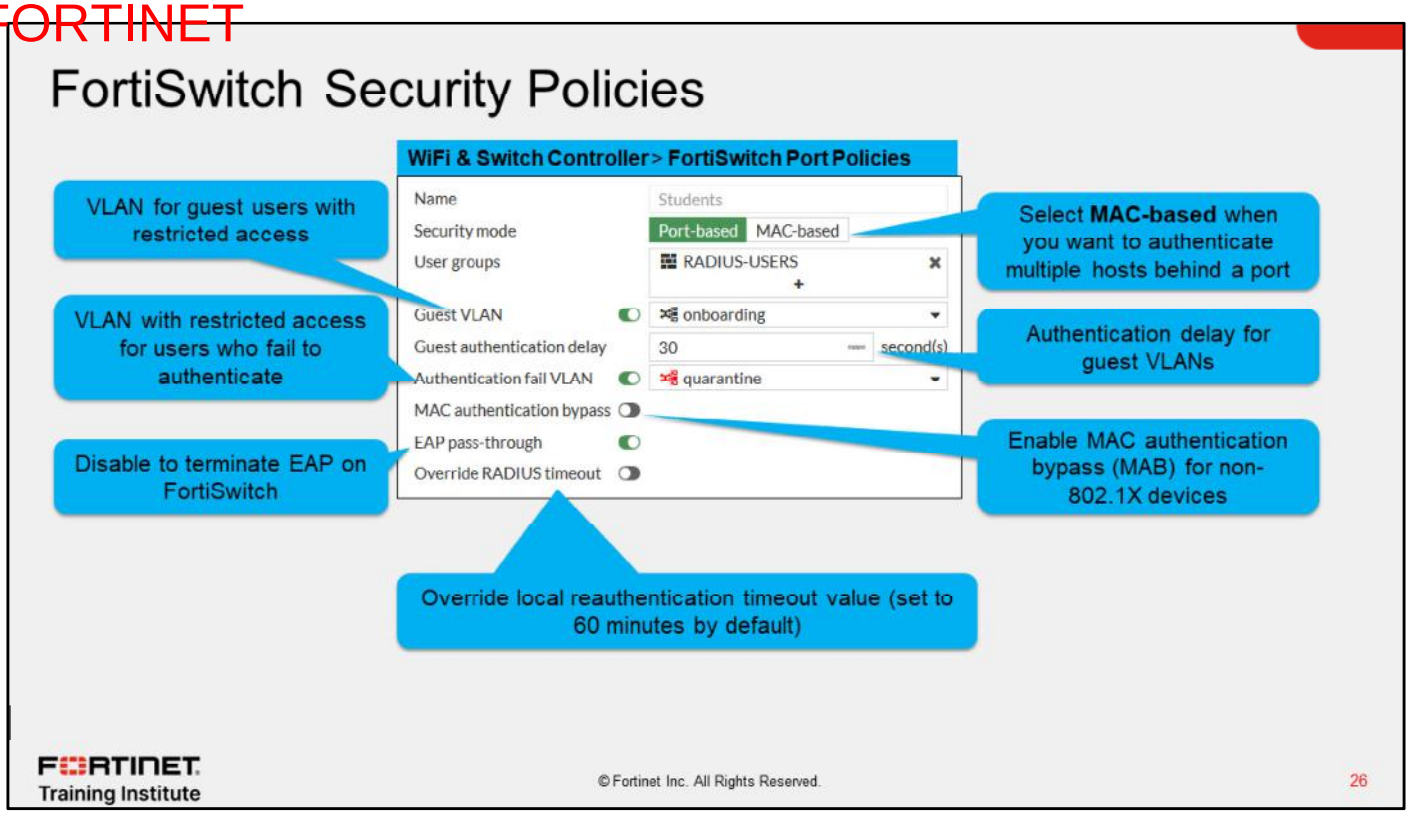
- The client, also known as the supplicant, is the device that wants to join the network. Its network stack must support 802.1X.
- The authenticator is a network device, such as a wireless access point or a switch, that acts as the broker in the authentication process. The authenticator allows or denies network access to the supplicant based on the response received from the authentication server.
- The authentication server is a host that supports RADIUS and EAP, such as FortiAuthenticator, and that verifies the client credentials. The client credentials can be a username and password, or a digital certificate. The authentication server also grants the supplicant a level of network access based on the configured authentication policies.

The client is not allowed to access the network until the client credentials are validated and authorized. Using 802.1X authentication, the client provides their credentials to the authenticator, which then passes the information on to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is granted access to the network.

Note that the authenticator does not need to store the client credentials or have knowledge of the authentication method (for example, PEAP or EAP-TLS). The authentication messages are tunneled from the client to the authentication server over the RADIUS protocol.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



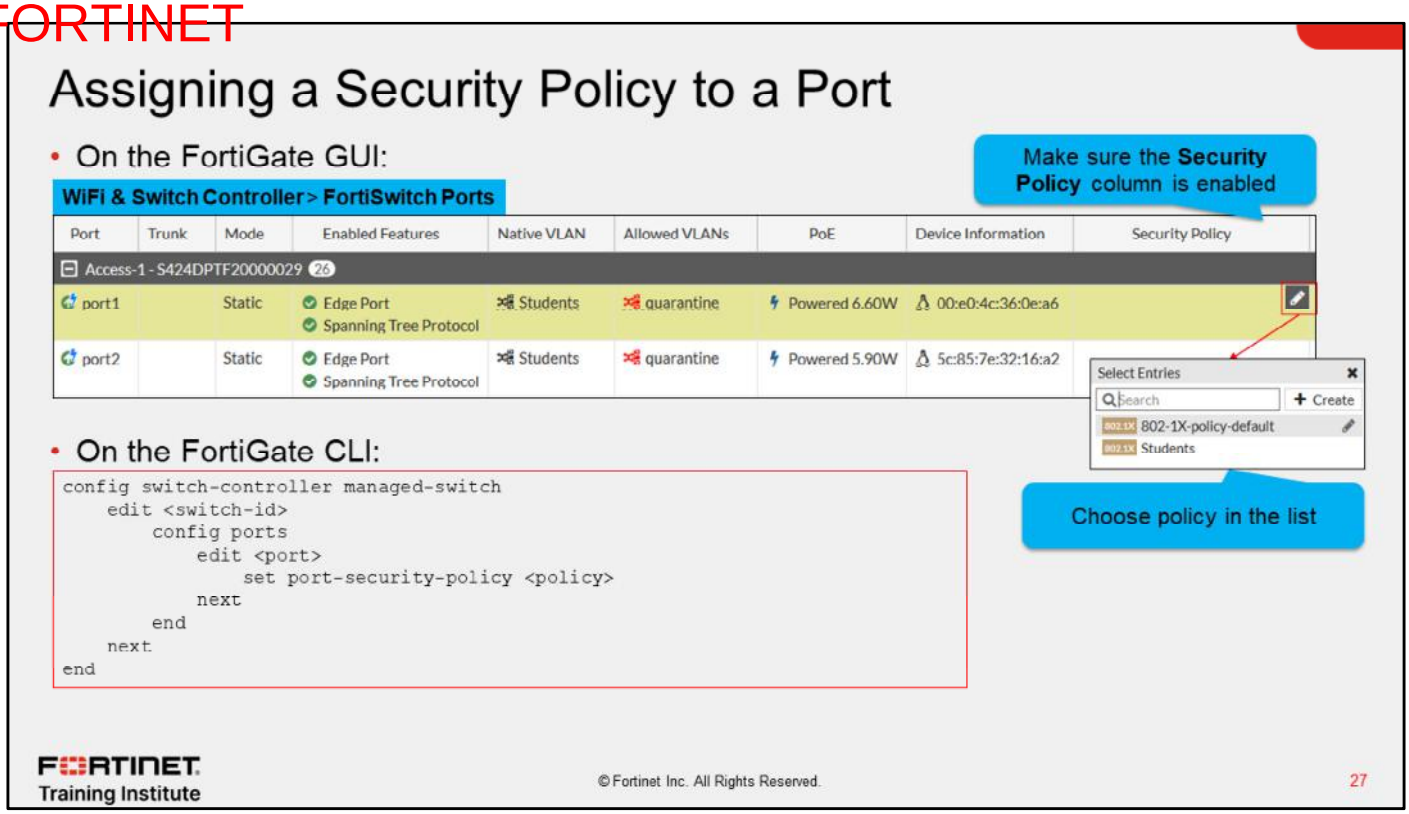
To configure 802.1X authentication on FortiSwitch, you must first create a security policy. When you configure a security policy, you must select **Port-based** or **MAC-based** in the **Security mode** field. **Port-based** is preferred when you expect a single host per port to authenticate, even though there may be multiple hosts connecting to the same port. Under this scenario, FortiSwitch authenticates a single host, and opens the port to other devices behind the port. A use case for this scenario could be an access point (AP). After the AP authenticates against the switch, any of its connected devices can access the network despite them using a different MAC address from the one used by the AP during authentication. In addition, all devices are granted the same access level assigned to the AP. However, if you want to authenticate each device behind a port, and optionally, grant each device a different access level based on the credentials provided, then **MAC-based** is required. Security-wise, MAC-based is preferred because each host (or MAC address) behind the port must authenticate for accessing the network. Performance-wise, port-based is better because only a single host is required to authenticate.

If a device does not support 802.1X, you can configure the security profile to place that device in the VLAN selected as **Guest VLAN**. Alternatively, you can enable **MAC authentication bypass** to allow access to a non-802.1X device, provided the device MAC address is authorized on the authentication server. You can also place devices that try to authenticate through 802.1X, but fail, in the VLAN selected as **Authentication fail VLAN**.

When **EAP pass-through** is enabled, EAP messages are forwarded to the authentication server. However, if the authentication server (RADIUS server) does not support EAP, or you want FortiSwitch to authenticate users against its local user database, you should disable **EAP pass-through**. As an 802.1X authentication server, FortiSwitch supports EAP-PEAP, EAP-TTLS, EAP-TLS, and EAP-MD5. Finally, if you enable **Override RADIUS timeout**, the switch overrides the local reauthentication timer with the session-timeout attribute value received from the RADIUS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

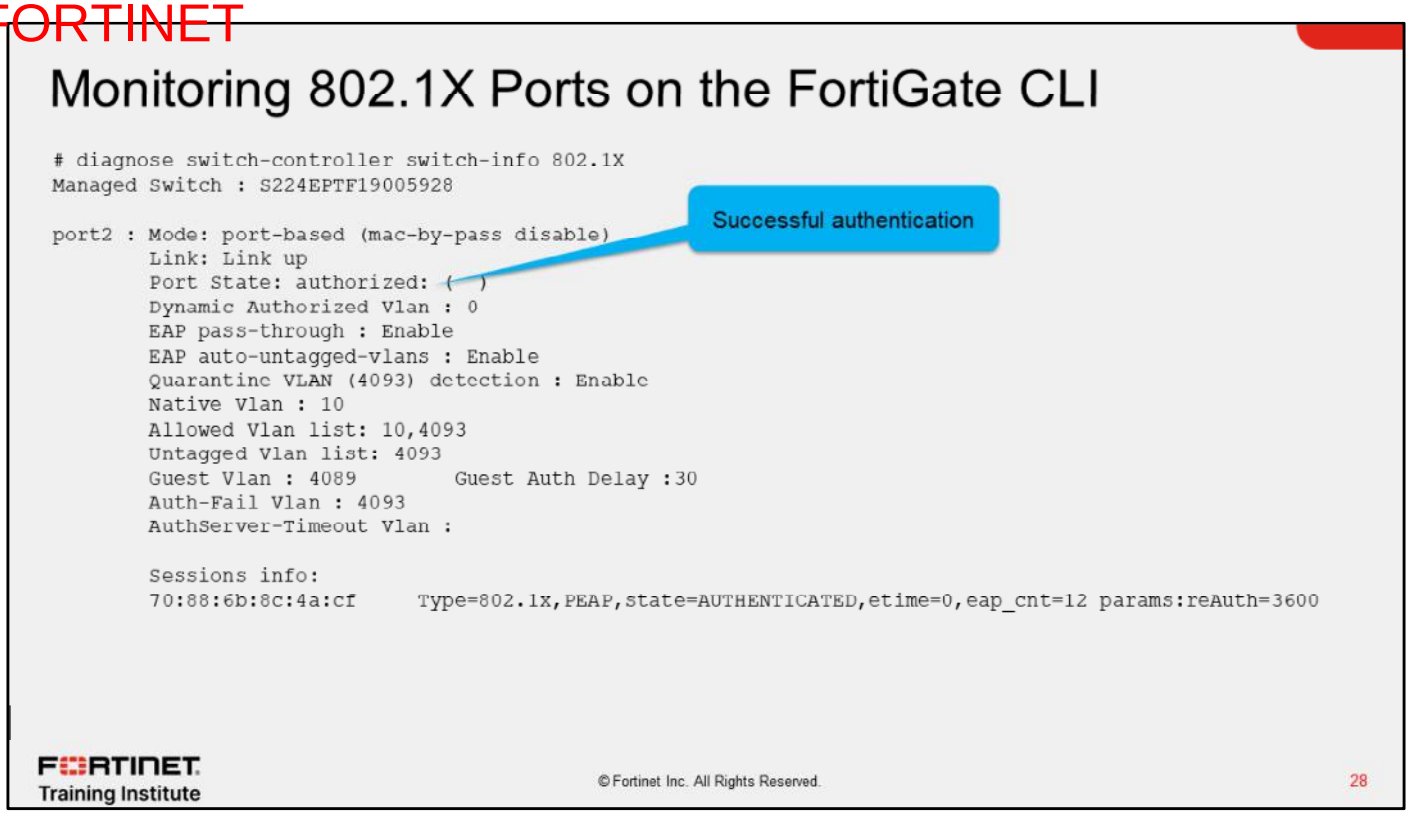
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After creating a security policy, you can assign it using the FortiGate GUI or CLI as shown on this slide. When using the FortiGate GUI, ensure that the **Security Policy** column is visible. 802.1X authentication is enforced only on ports assigned with a security policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

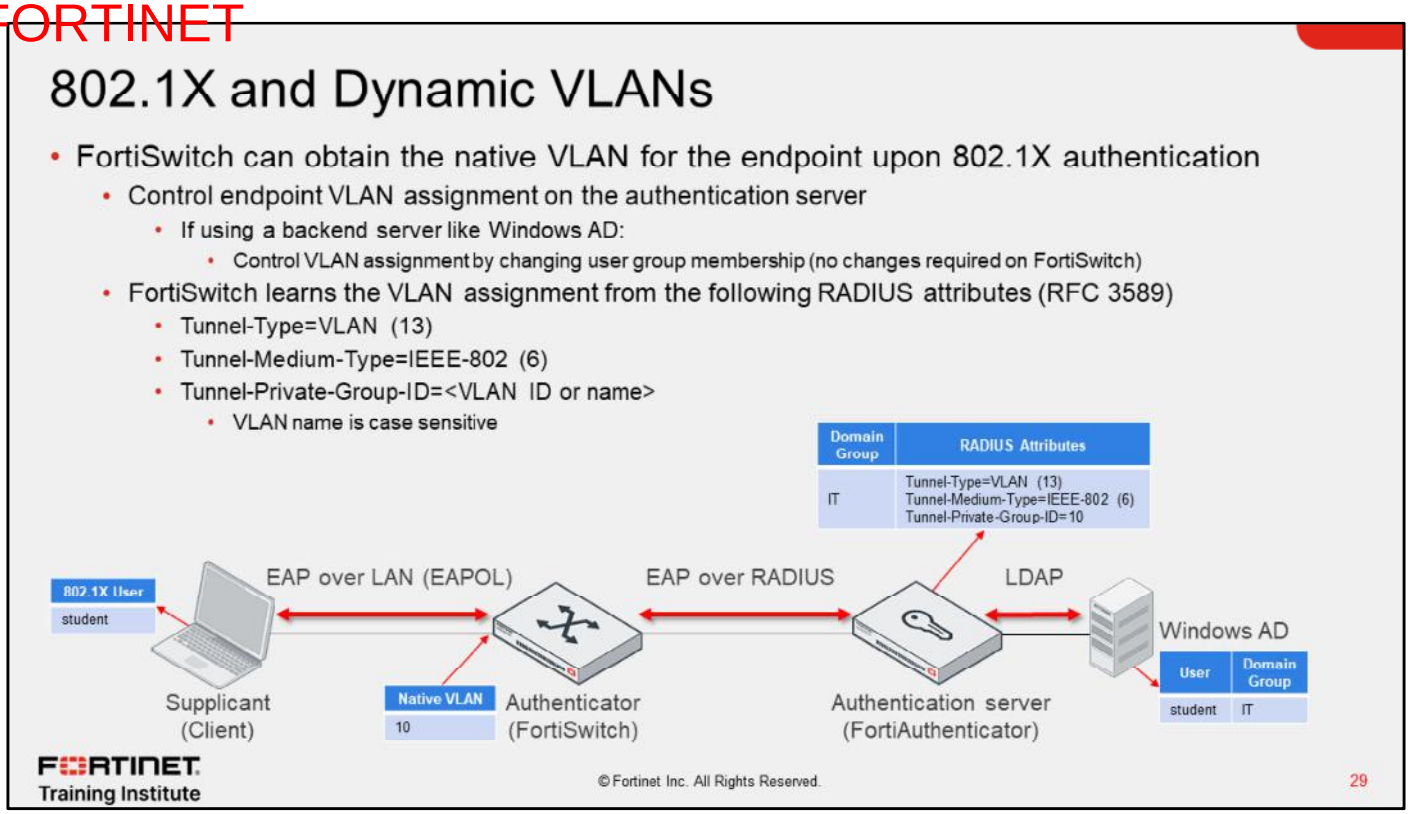
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiGate CLI command on this slide displays the 802.1X status for each switch port performing 802.1X authentication. The output indicates the 802.1X security mode in use, whether the device is authorized or not, as well as the EAP method in use. The output also shows important information, such as the device MAC address, quarantine VLAN, native VLAN, allowed VLANs, guest VLAN, and authentication fail VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



One benefit of using 802.1X is that FortiSwitch can also get the native VLAN for an endpoint from the authentication server upon a successful authentication. This enables the administrator to dynamically assign VLANs to endpoints by making changes in the authentication server only, and without requiring any further changes on FortiSwitch.

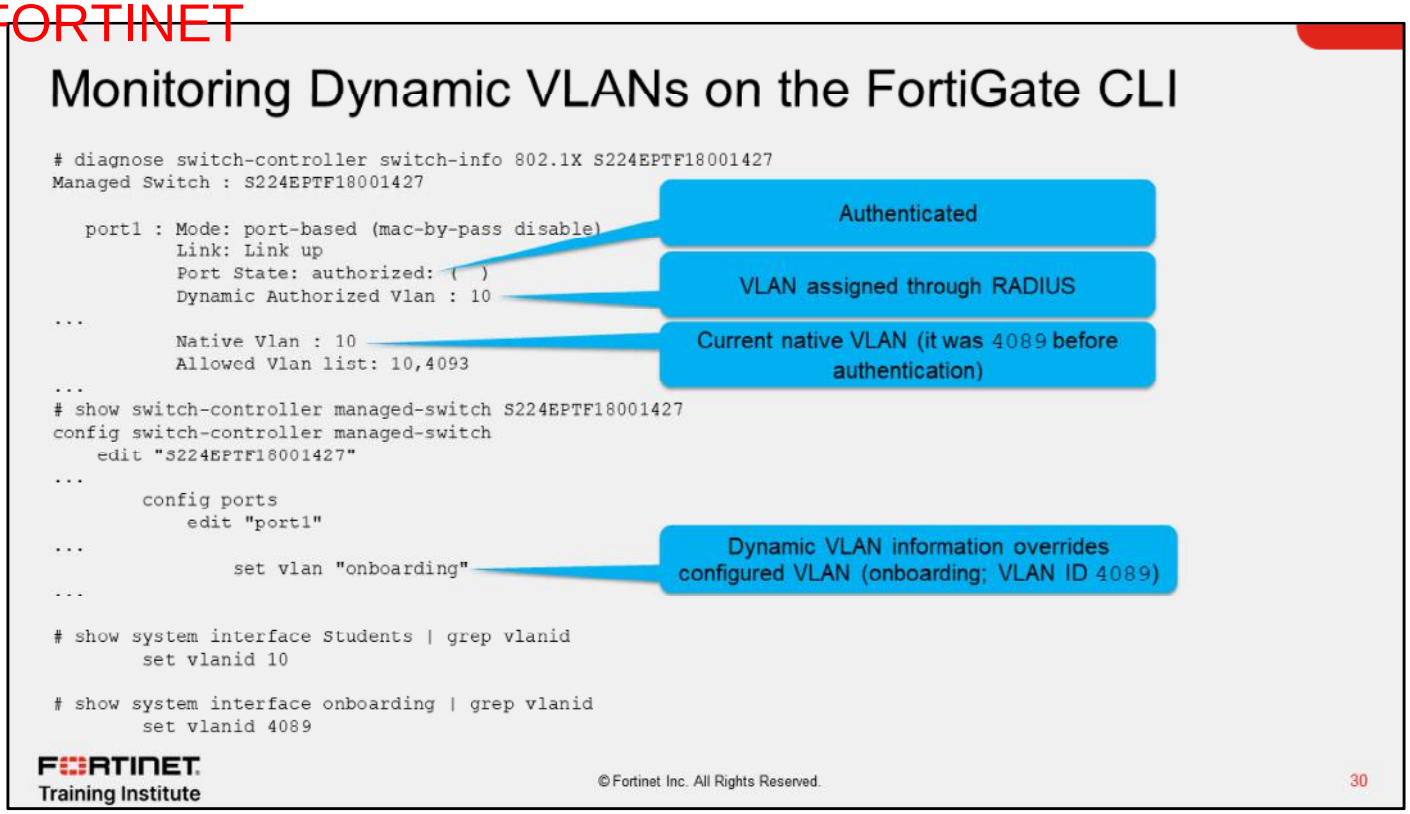
The deployment becomes even more scalable if you configure your authentication server to authenticate 802.1X users against a backend server, such as Windows AD, that contains all existing domain users in the network. You could then configure rules in the authentication server to map domain user groups to VLANs. The result is that FortiSwitch can automatically assign the VLAN for an endpoint based on the domain user group that the 802.1X user belongs to. This means that you can control the VLAN assignment on endpoints just by changing the user group membership on the backend server.

For FortiSwitch to learn the VLAN information during 802.1X authentication, it must receive the three RADIUS attributes shown on this slide, and defined in RFC 3589, from the authentication server. Note that you can indicate the VLAN ID or the FortiSwitch VLAN name as Tunnel-Private-Group-ID. If you want to indicate the VLAN name, ensure that it is written exactly as configured on FortiGate.

The example on this slide shows that FortiSwitch assigns the client to VLAN 10 because FortiAuthenticator is configured to return the RADIUS attribute Tunnel-Private-Group-ID=10 to FortiSwitch upon authentication. FortiAuthenticator returns that attribute because it determines that the 802.1X user—student—is a member of the IT domain user group by querying the user group membership information from the Windows AD backend server using LDAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



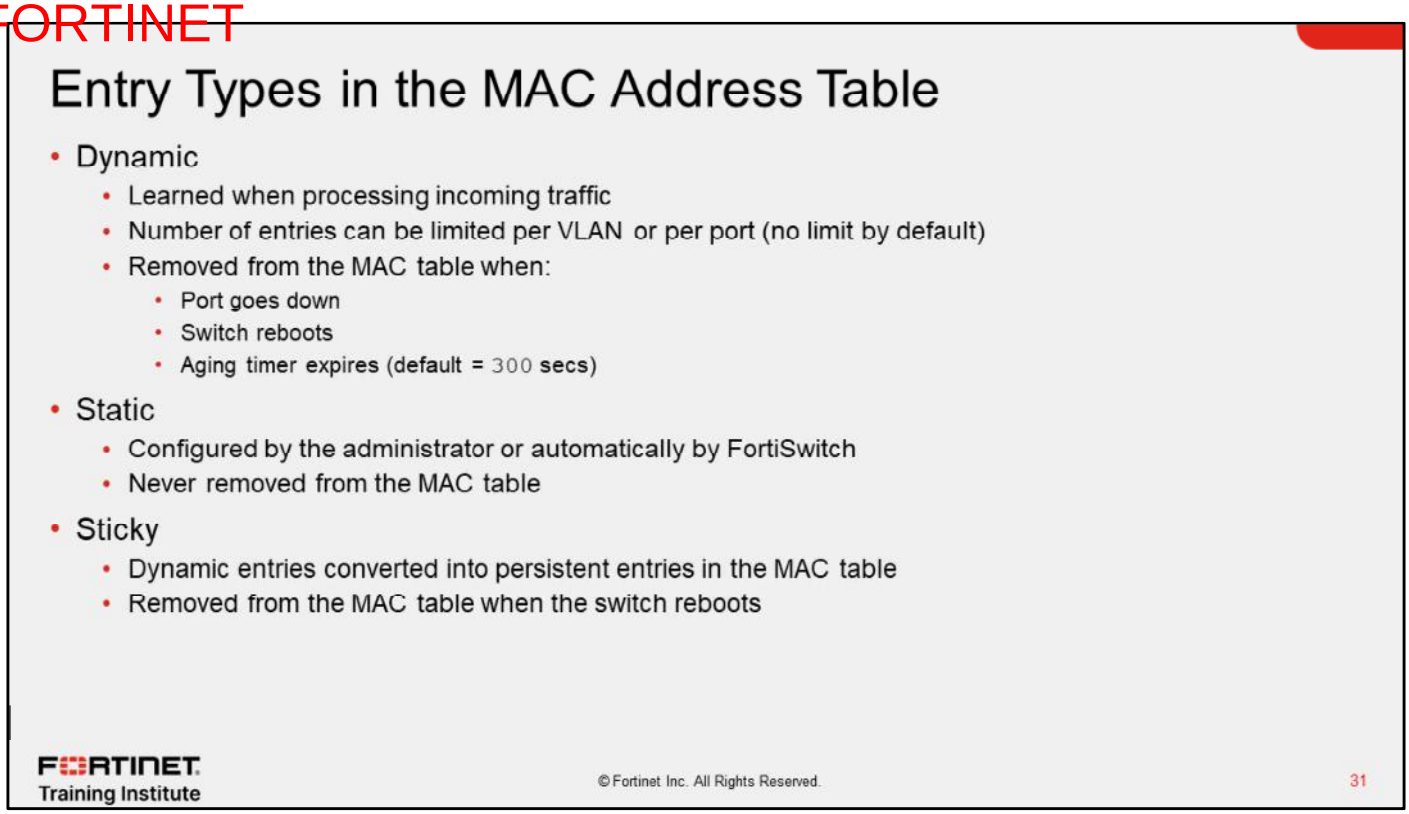
You can use the FortiOS 802.1X status command for managed switches to view the VLAN assigned to 802.1X ports through RADIUS.

The example on this slide shows the output from the 802.1X status command on FortiOS, as well as the switch port involved and the FortiSwitch VLAN configuration. Some irrelevant lines have been removed from the output so it can fit on this slide. The output shows that the VLAN ID (`10`) on `Dynamic Authorized Vlan` is different from the VLAN ID (`4089`) configured on the FortiSwitch VLAN (`onboarding`) assigned to the port. This means that FortiSwitch overrides the native VLAN configuration on a port, with the VLAN ID learned from the authentication server through RADIUS upon a 802.1X successful authentication.

You can also configure dynamic VLANs using other features, such as FortiOS integrated NAC, FortiSwitch ACLs, or FortiSwitch MAC-VLAN binding. However, none of these options are as scalable as using 802.1X authentication when it comes to dynamic VLAN assignment. You will learn more about these additional features in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



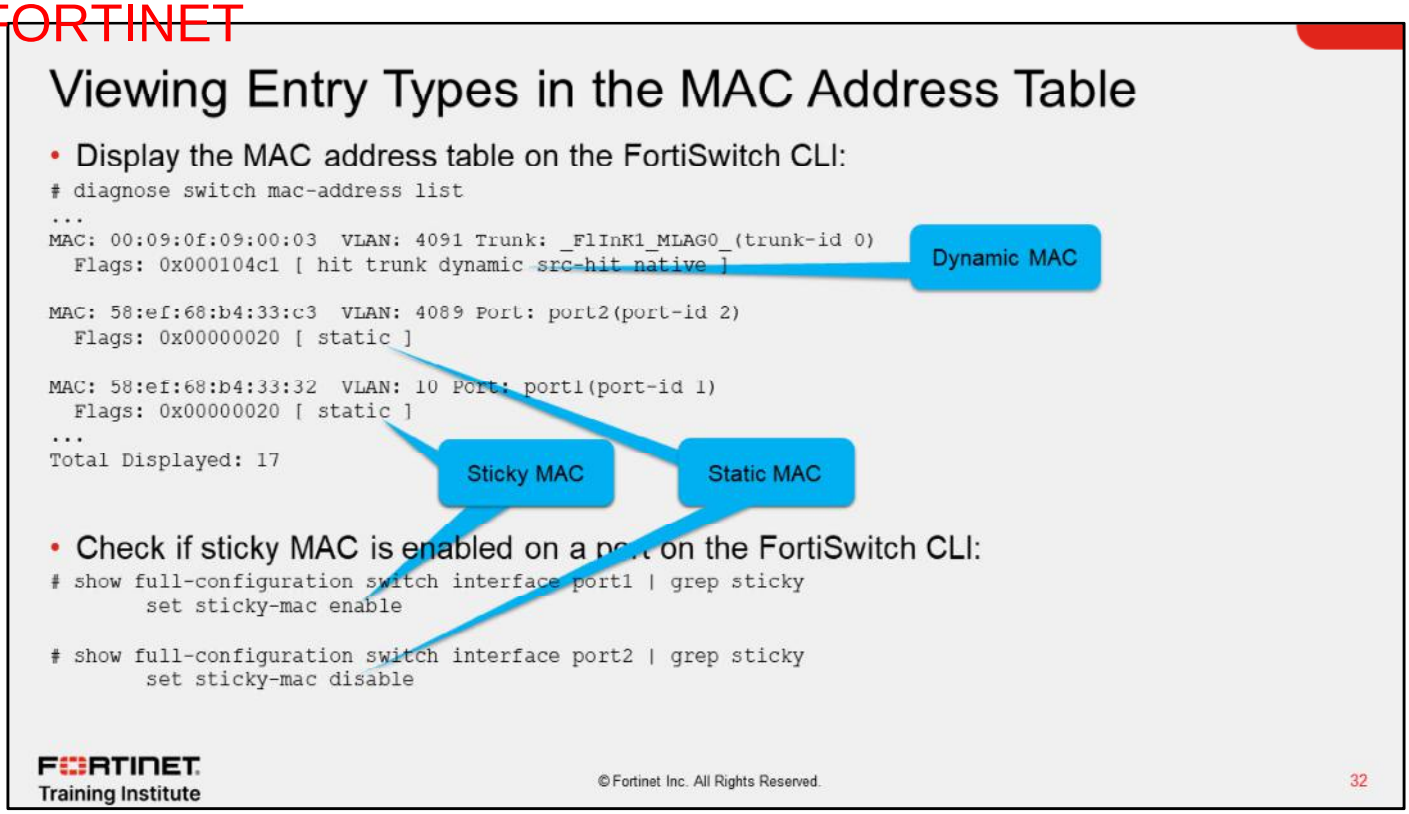
The MAC address table on FortiSwitch is composed of dynamic and static entries. Dynamic entries are learned when FortiSwitch processes incoming traffic, while static entries are either configured by the administrator or automatically created by the switch.

By default, there is no limit on the number of dynamic MAC addresses that FortiSwitch can learn on a port. However, you can limit the number of dynamic entries on a VLAN or on a port for security reasons. Dynamic entries are removed from the MAC address table when a port goes down, when a switch reboots, or when their aging timer expires—300 seconds by default. If you want FortiSwitch to always list a MAC address on a specific port, you can configure a static entry on FortiSwitch for that MAC address and port.

There is another type of MAC address you can configure on FortiSwitch: a sticky MAC address. Sticky MAC addresses are dynamic entries that are converted into persistent entries in the MAC address table. However, unlike static entries, which are kept in the MAC address table during a port status change or a switch reboot, sticky MAC addresses are only retained when a port goes down. If FortiSwitch reboots, sticky MAC addresses are removed from the MAC address table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

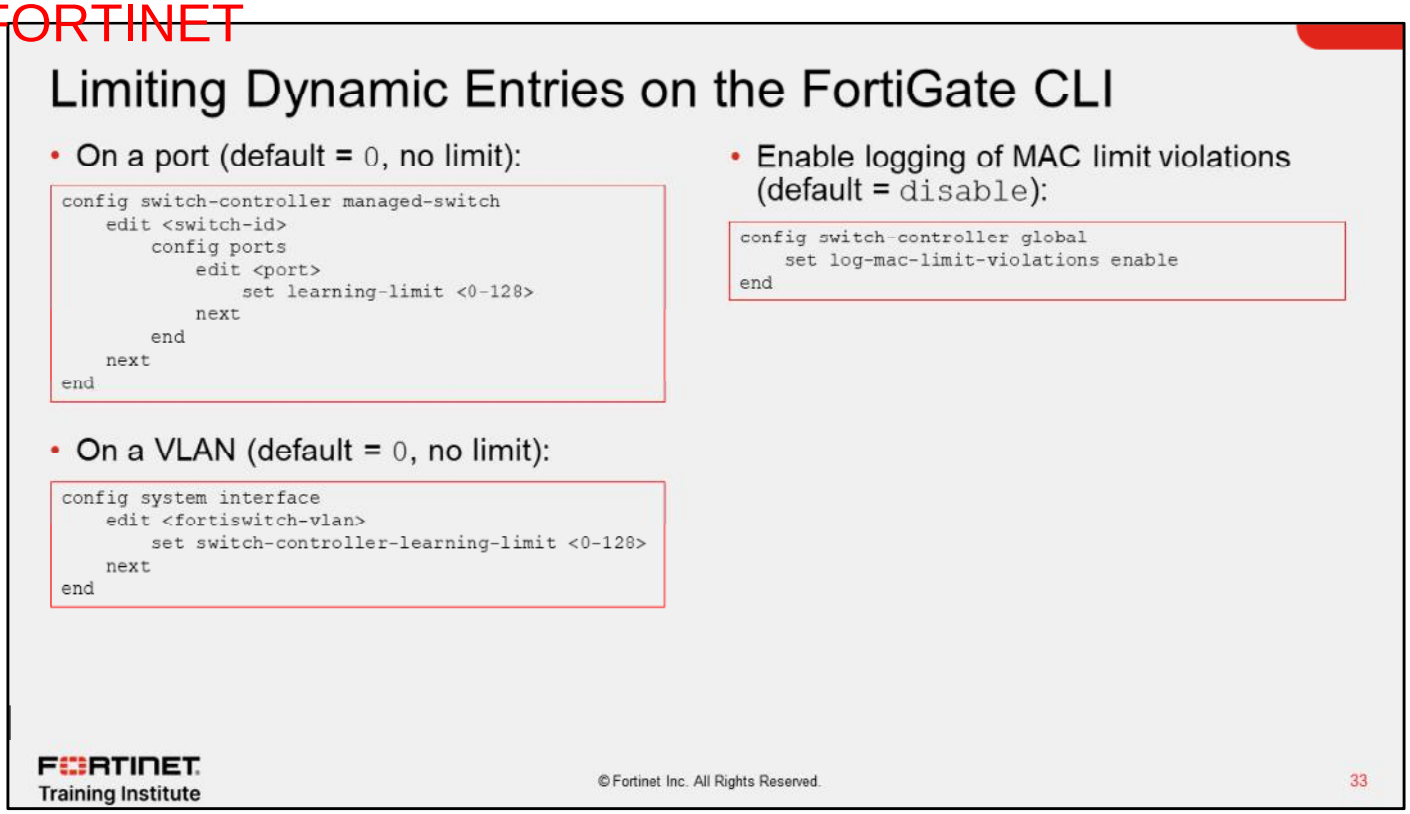


The entry type in the MAC address table is indicated only when you display the MAC address table directly on the FortiSwitch CLI by using the command shown on this slide.

Note that both static and sticky MAC address entries are displayed as `static` in the MAC address table on the FortiSwitch CLI. However, you can tell if the MAC address is sticky if the port has the `sticky-mac` setting enabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

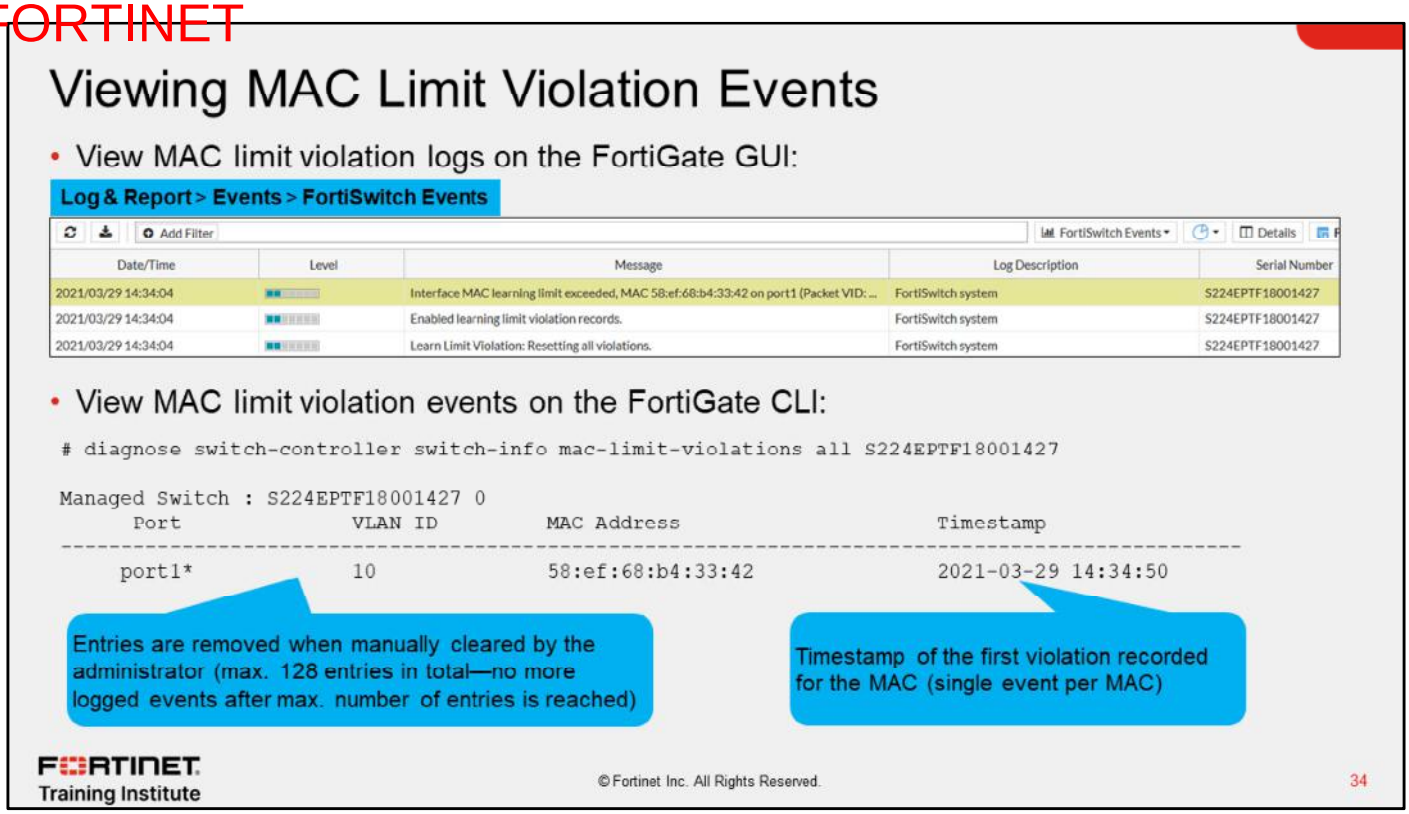


You can limit the number of dynamic MAC address entries learned on a port or on a VLAN by running the commands shown on this slide. By default, the limit is set to 0, which means there is no limit.

By default, FortiSwitch does not log an event when the number of dynamic entries seen on a port or on a VLAN exceeds the configured limit. You can enable the logging of MAC limit violations by running the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



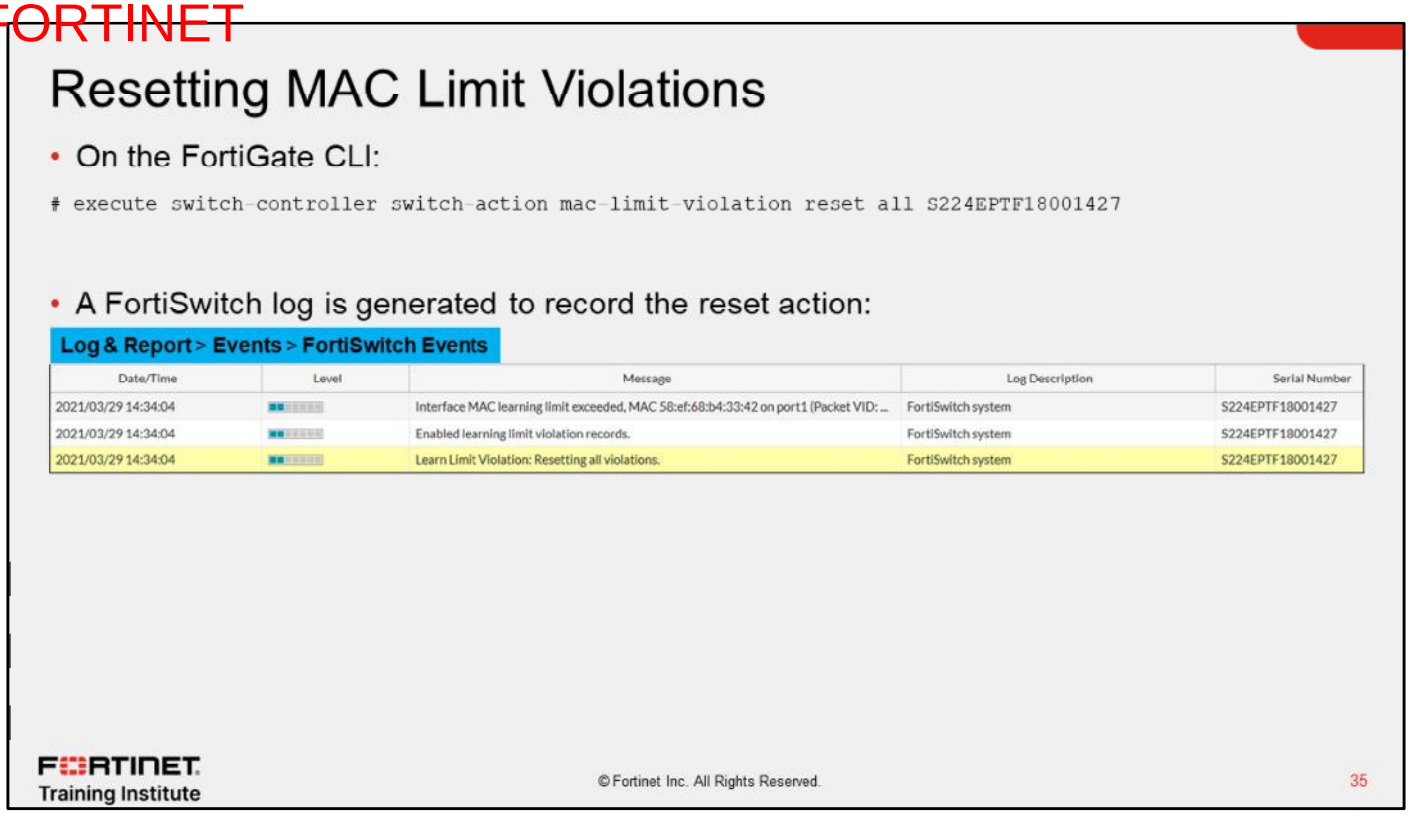
You can view MAC limit violation logs on the FortiGate GUI by browsing to the **FortiSwitch Events** subcategory.

In addition to logs, FortiSwitch also keeps a list of MAC limit violations. You can view this list on the FortiGate CLI by running the command shown on this slide. The timestamp shown for each event corresponds to the time of the first recorded violation. The list shows a single event per MAC address, even if FortiSwitch has blocked multiple packets from that MAC address.

Note that the list supports up to 128 entries in total. No additional events are logged once the maximum number of entries is reached. However, you can reset the events.

Vouchers & Dumps are Available | WhatsApp +201224560923

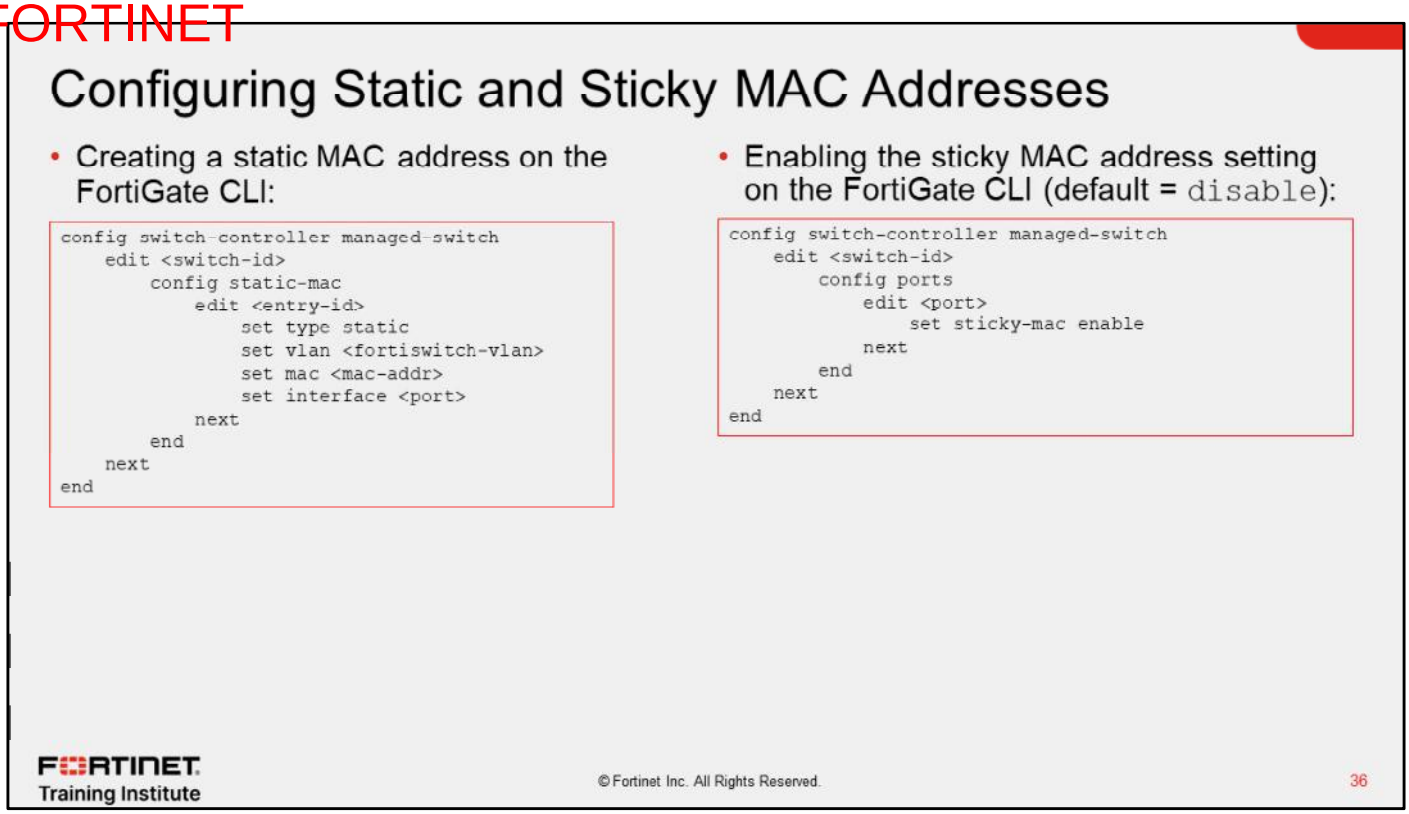
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can reset the recorded MAC limit violations by running the FortiGate CLI command shown on this slide. When you reset the MAC limit violations, FortiSwitch generates a log to record the reset action.

Vouchers & Dumps are Available | WhatsApp +201224560923

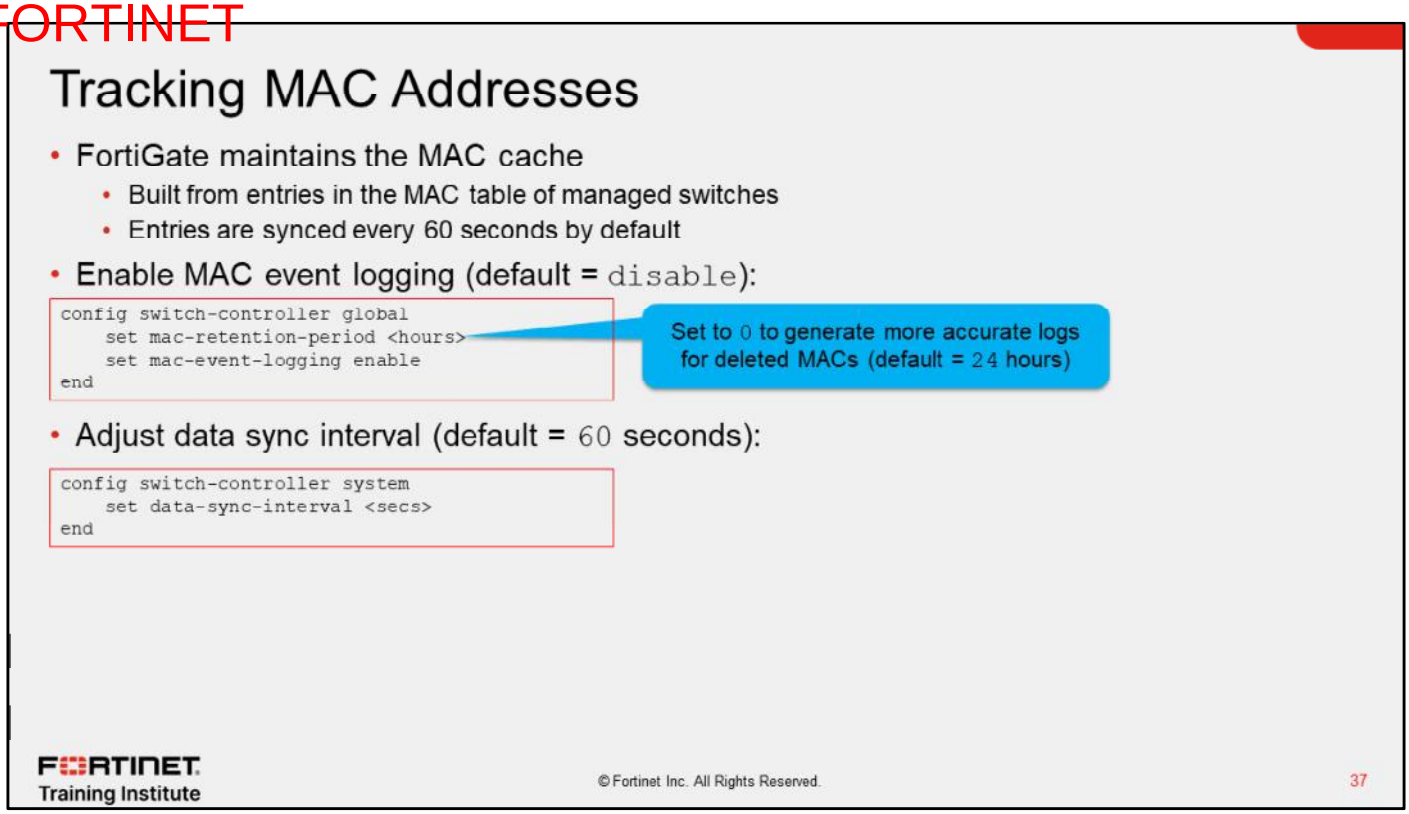
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can create static MAC address entries by running the commands shown on this slide. To enable sticky MAC on a port, enable the `stick-mac` setting on the port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate maintains a MAC cache that is built from the entries in the MAC address table of managed switches. FortiGate synchronizes the entries from the managed switches every 60 seconds by default. FortiGate can then log any changes in the MAC cache contents so the administrator can keep track of the MAC addresses that have been discovered or deleted by switches.

You can enable the logging of MAC events by running the commands shown on this slide. Discovered MAC addresses are logged by FortiGate within 60 seconds—the default data sync interval—after being added in the FortiSwitch MAC address table. However, deleted MAC addresses are kept in the MAC cache for 24 hours by default, even though they are no longer present in the MAC address table of FortiSwitch. If you want FortiGate to log a message for a deleted MAC within 60 seconds of disappearing from the network, you can set the MAC retention period to `0`.

The default 60-second data sync interval works fine for most deployments. You can still adjust the timer by running the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Tracking MAC Addresses (Contd)

- View discovered and deleted MAC addresses on the FortiGate GUI:

Log & Report > Events > FortiSwitch Events

Date/Time	Level	Message	Log Description	Serial Number
2021/03/30 06:47:28		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 06:38:28		58:ef:68:b4:33:c3 discovered on interface port2 in vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 06:27:28		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 06:05:26		58:ef:68:f4:00:00 discovered on interface port2 in vlan 4089 on Switch S224EPTF180014...	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 06:04:26		58:ef:68:b4:33:c3 deleted from vlan 4089 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 06:04:26		58:ef:68:b4:33:c3 discovered on interface port2 in vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 06:02:26		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 05:55:26		58:ef:68:b4:33:c3 discovered on interface port2 in vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 05:02:23		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 04:55:22		58:ef:68:b4:33:c3 discovered on interface port2 in vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 04:02:20		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427
2021/03/30 03:55:19		58:ef:68:b4:33:c3 discovered on interface port2 in vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC add	S224EPTF18001427
2021/03/30 03:02:16		58:ef:68:b4:33:c3 deleted from vlan 10 on Switch S224EPTF18001427	FortiSwitch MAC delete	S224EPTF18001427

FORTINET Training Institute

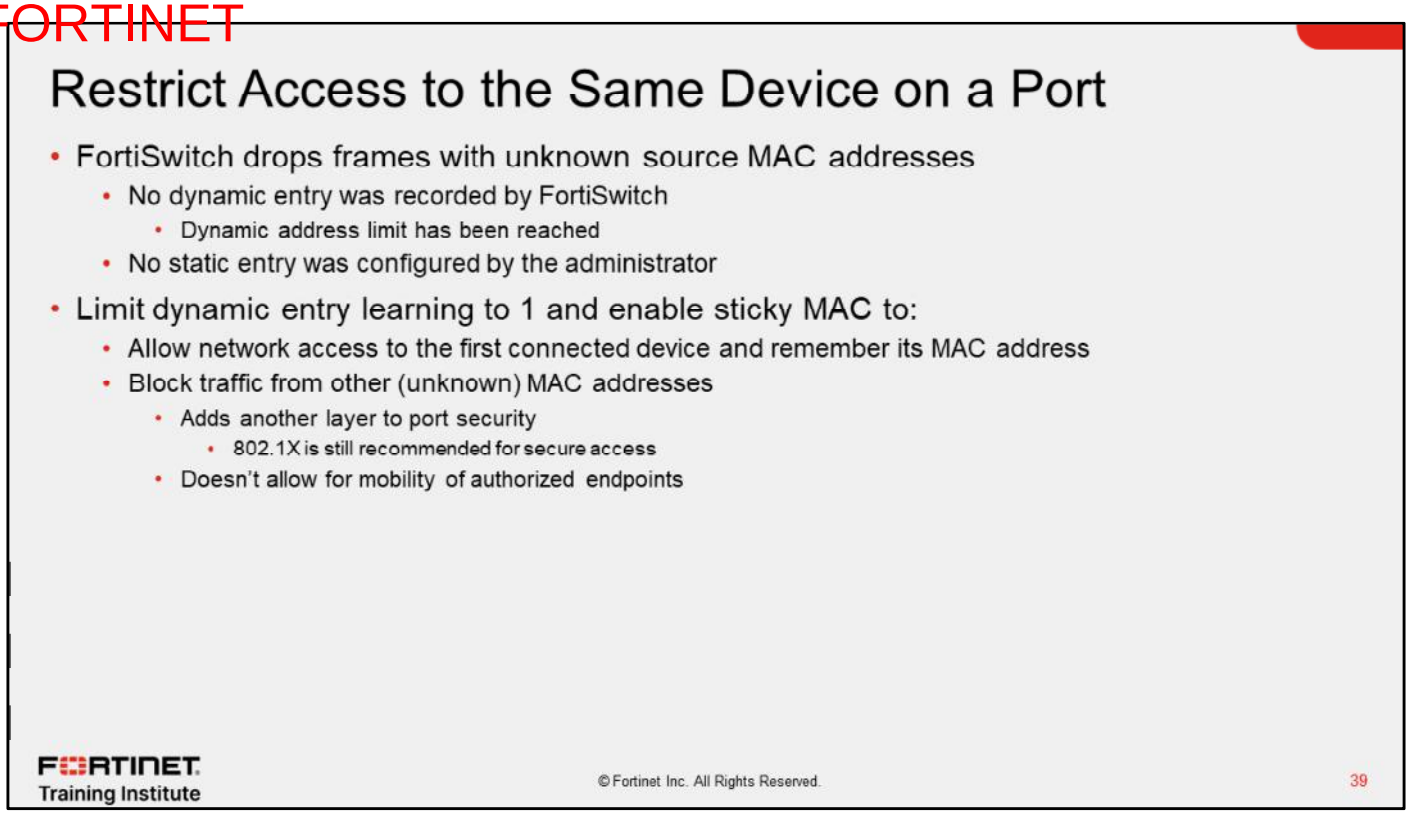
© Fortinet Inc. All Rights Reserved.

38

After you enable the logging of MAC events, FortiGate begins generating logs for every MAC address that is added or removed from its MAC cache. You can view these logs on the FortiGate GUI by browsing to the **FortiSwitch Events** subcategory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSwitch forwards frames based on the destination MAC address in the frame. However, before forwarding the frame, FortiSwitch checks whether an entry for the source MAC address in the frame was added, either dynamically or statically, to the MAC address table. If there is a limit to the dynamic entries learned on a port or on a VLAN, and the limit has been reached, FortiSwitch is unable to add a dynamic entry for the source MAC address in the MAC address table. Also, if the administrator didn't configure a static entry for the source MAC address in the MAC address table, there won't be a static entry for the source MAC address either. The result is that FortiSwitch drops the frame.

Because of the previous behavior, you can configure FortiSwitch to accept traffic from the first device—the first MAC address—that is connected to a port and drop traffic from other MAC addresses seen on the port. In many cases, the first device that is connected to a port is the trusted device assigned to the user. For this reason, you may want to ensure that FortiSwitch accepts traffic on the port only if it comes from that device. You can achieve this by limiting the number of dynamic entries learned on a port to 1, and then enabling sticky MAC on the port. When you enable sticky MAC on a port, FortiSwitch makes dynamic MAC addresses learned on a port persistent in the MAC address table during port status changes. The result is that the only traffic that FortiSwitch allows on the port is traffic from the MAC address that was originally connected to the port.

The previous configuration is a simple way for administrators to prevent users from connecting unauthorized devices to the network. However, it is by no means a way to provide secure access to network devices, or replace 802.1X authentication. For this reason, the setup should be seen as another layer that you can add to your port security deployment. A downside of this setup is that it doesn't allow for mobility of authorized endpoints in the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about 802.1X authentication is true?
   - A. FortiSwitch uses LDAP when communicating with the authentication server.
   - ✓ B. You can leverage 802.1X to dynamically assign the native VLAN of an authenticated device.

2. How can you view the entry type of an entry in the MAC address table of a managed switch?
   - ✓ A. By using the FortiSwitchOS `diagnose switch mac-address list` command.
   - B. By using the FortiOS `diagnose switch-controller switch-info mac-table` command.

3. Which statement about sticky MAC addresses is true?
   - A. The MAC address is kept in the MAC address table after the switch reboots.
   - ✓ B. The MAC address is kept in the MAC address table after the port goes down.

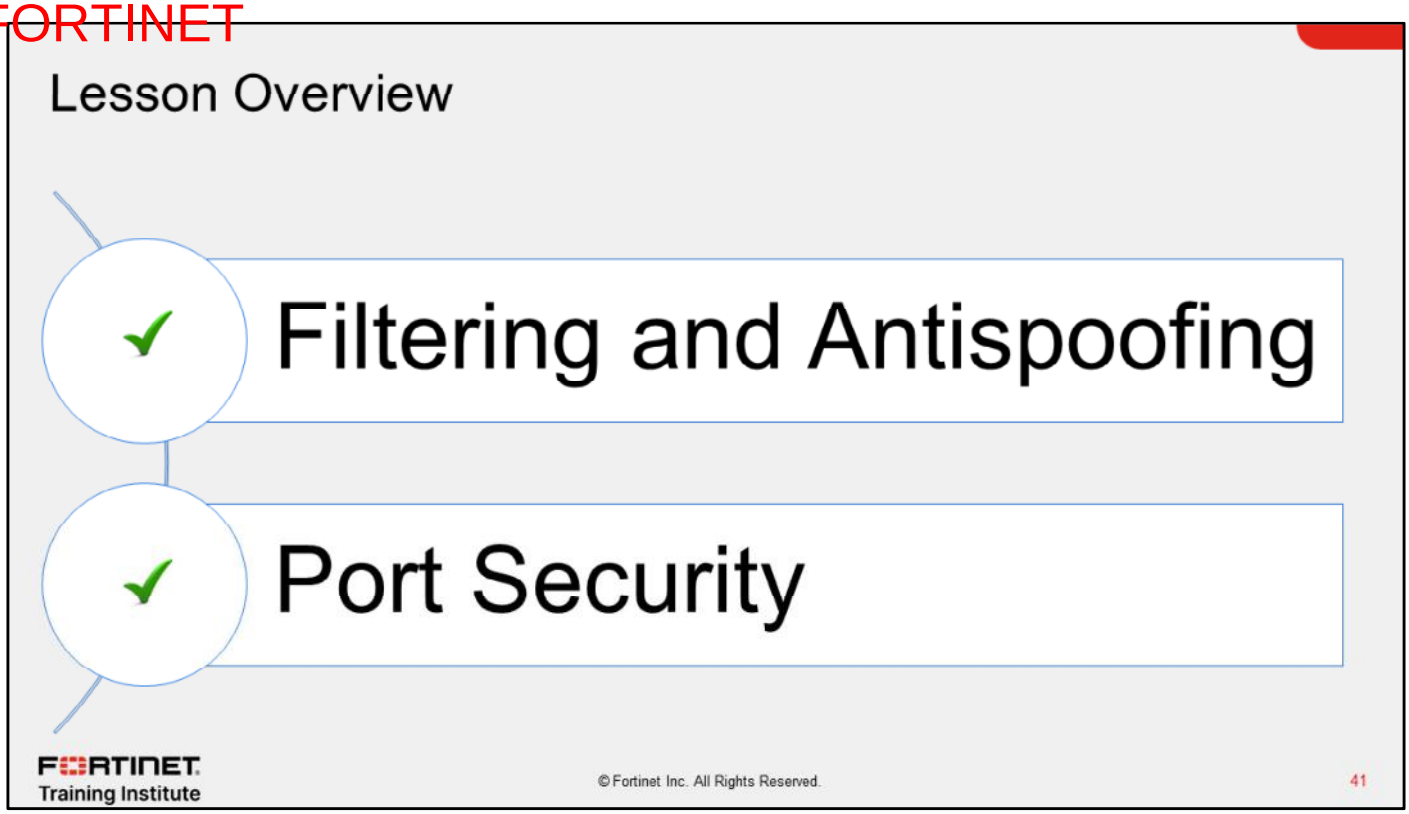
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

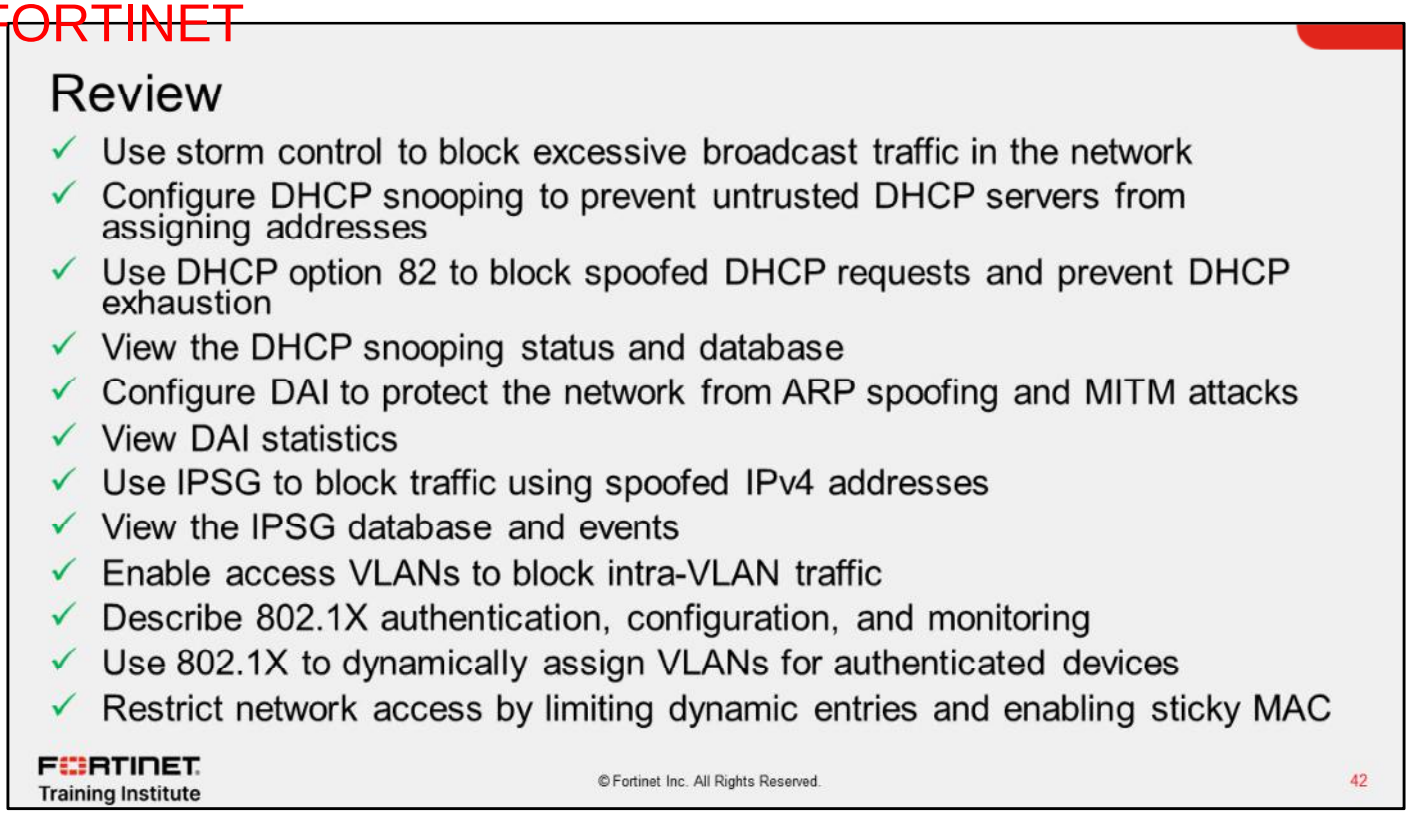


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

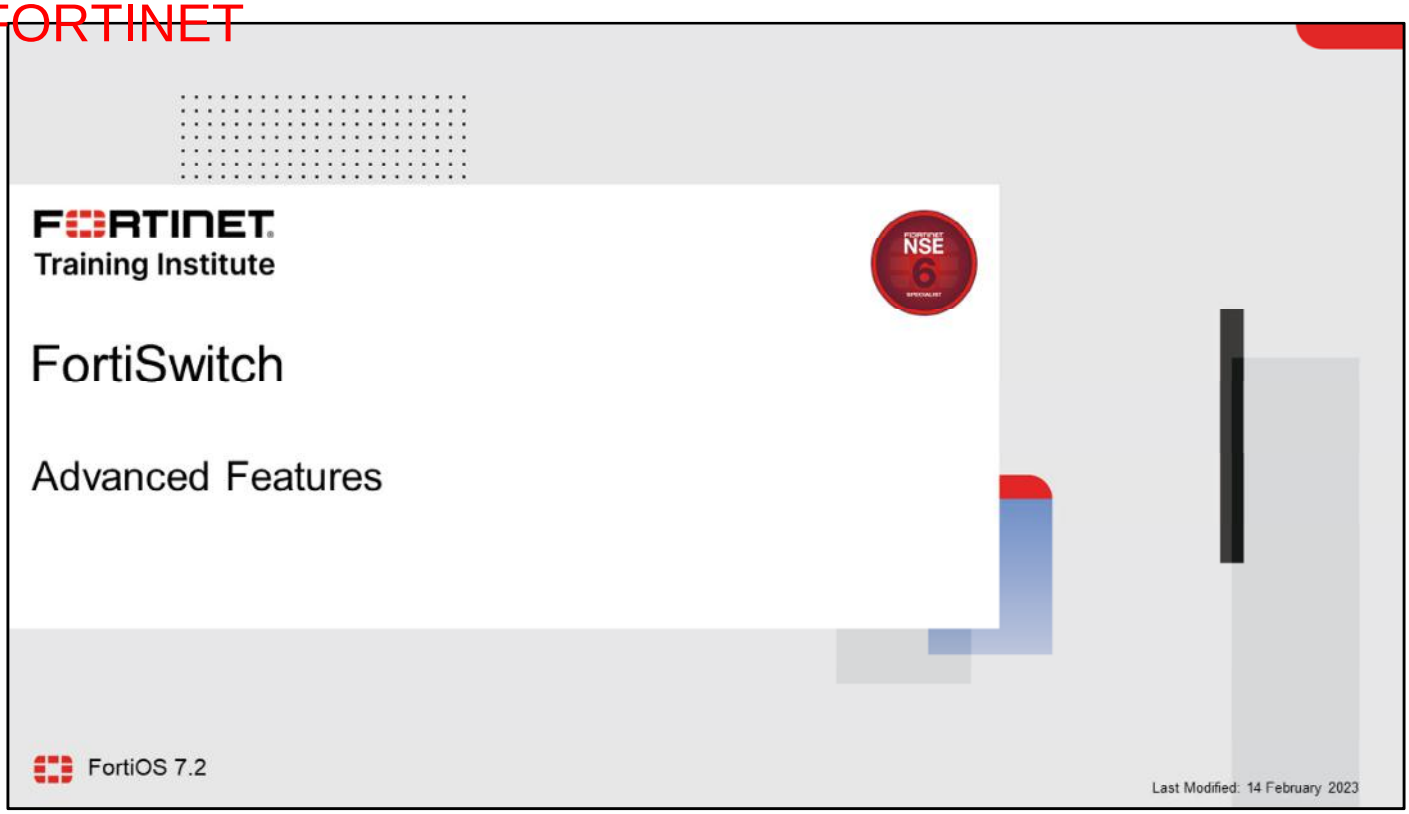


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the different security features that you can use to protect your network at Layer 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

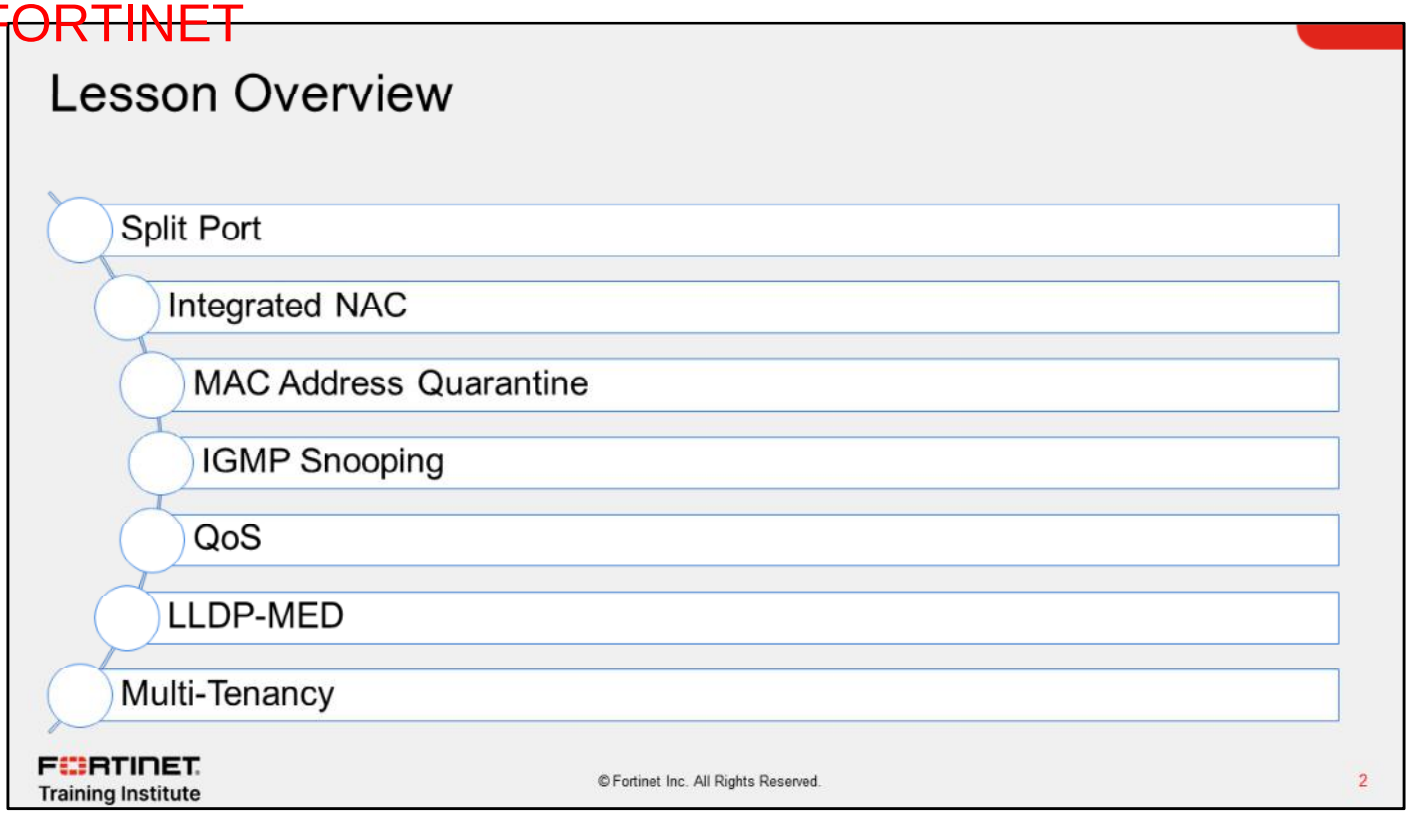
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about some of the advanced features available on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

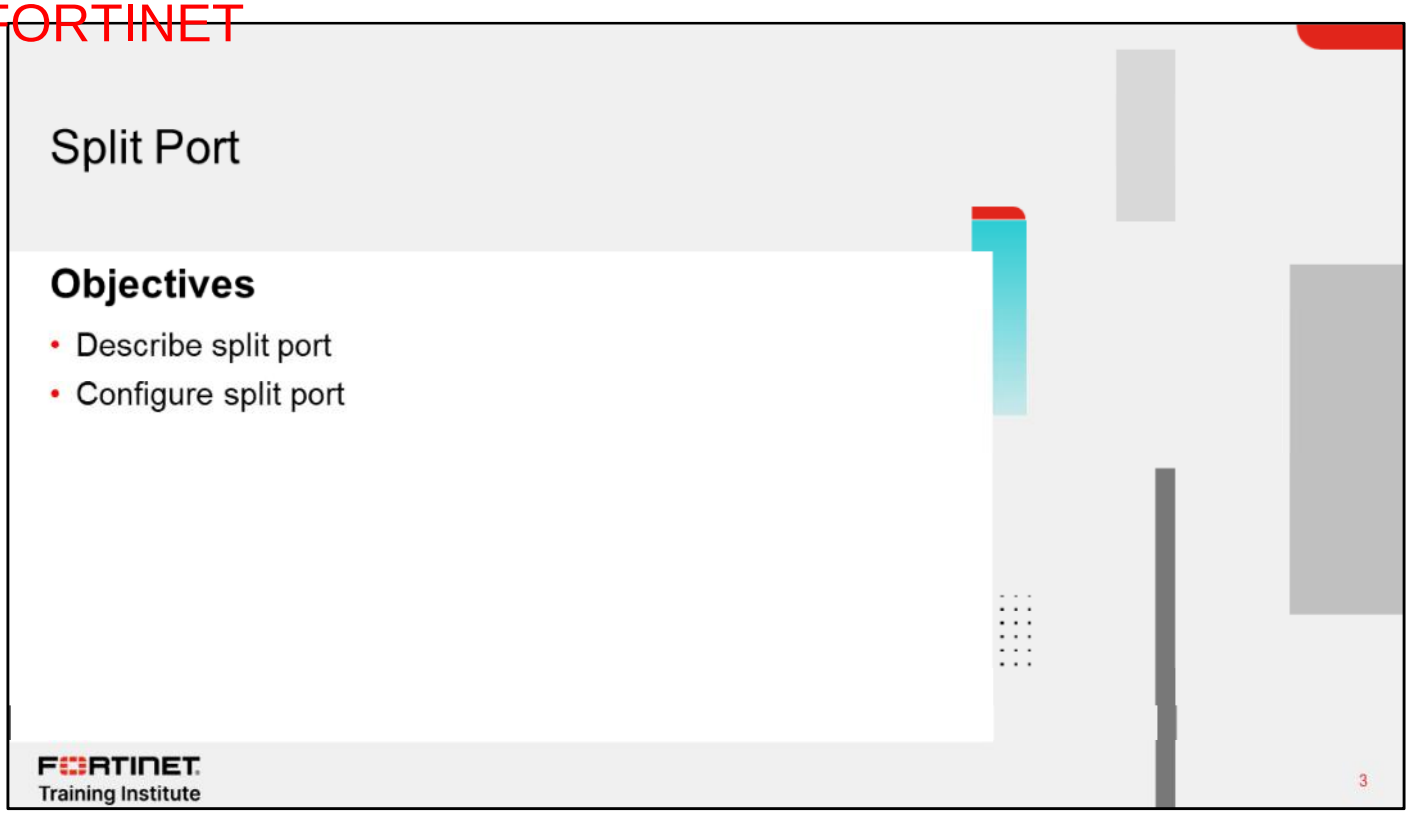
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using split port, you should be able to understand how to increase the port density on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

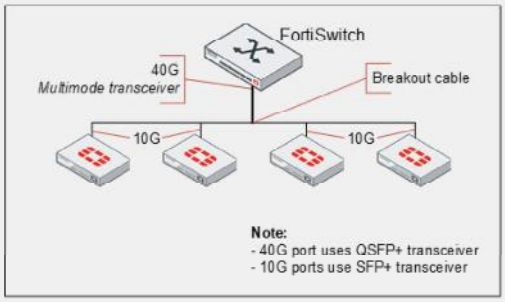
DO NOT REPRINT
© FORTINET
Brave-dumps.com

Split Port

- Converts 40G and 100G ports to 2–4 lower-speed ports
  - Requirements:
    - Compatible breakout cable
      - Refer to *FortiSwitch—Compatible Transceivers document* on `docs.fortinet.com`
    - Multimode transceiver
  - Increases port density on switch

FortiSwitch Split Port		
Port type	Speed	Split port modes
40G QSFP+	40G	4x10G/4x1G
100G QSFP28	100G	2x50G/4x25G/4x10G/4x1G *

* Model-dependent



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

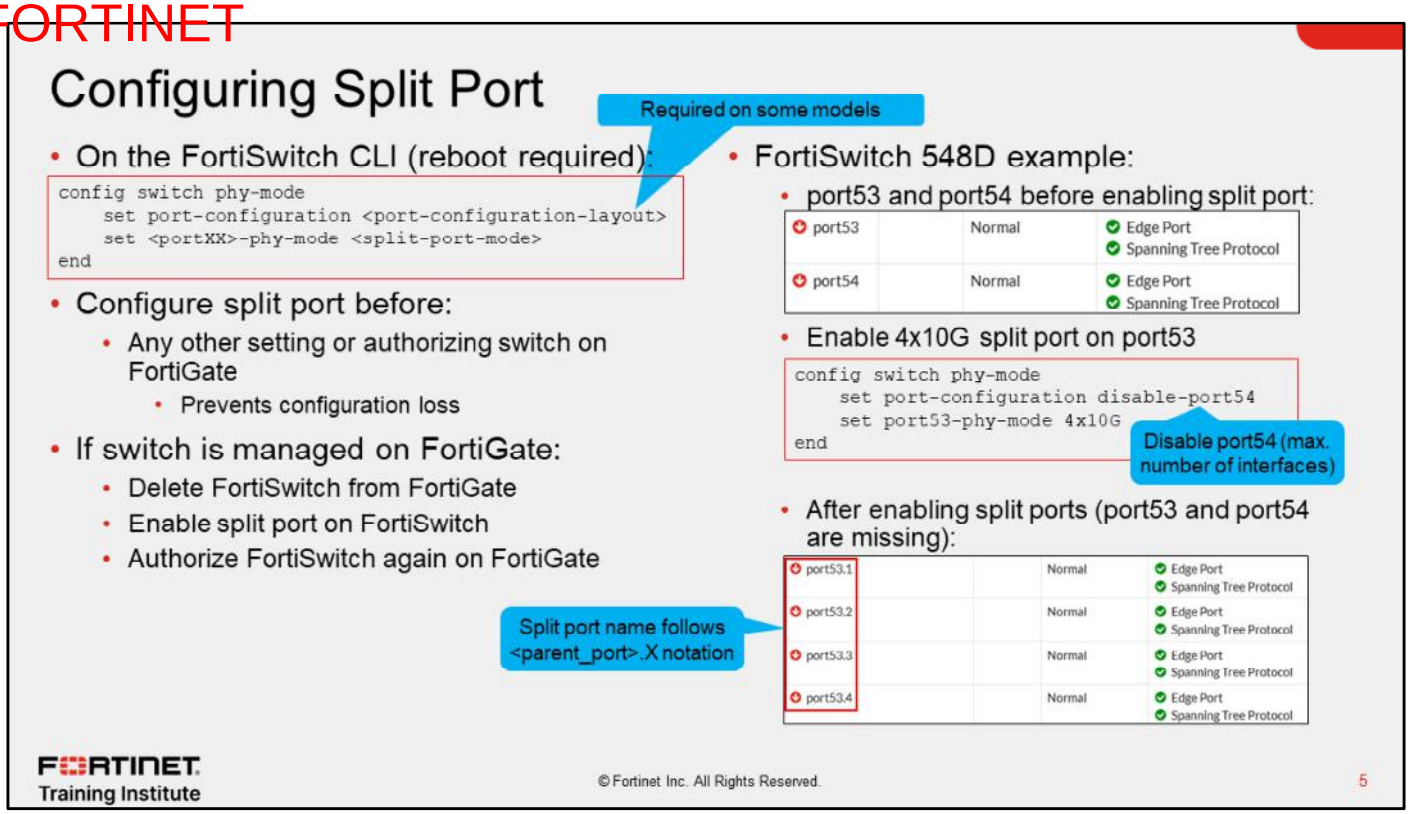
Split port enables you to use a breakout cable to convert a 40G or 100G port into multiple ports operating at lower speeds. Usually, you split a port because you need to increase the port density on your switch so you can connect more devices. For example, you can split a 100G port into four 25G ports, or a 40G port into four 10G ports. The table on this slide shows the split port modes supported by FortiSwitch for 40G and 100G ports.

To split a port, you must use the correct breakout cable and transceiver on FortiSwitch. For a list of compatible breakout cables (split cables), refer to the *FortiSwitch—Compatible Transceivers* document on `docs.fortinet.com`. For the transceiver, you must use a multimode transceiver because it uses four fiber pairs, which enables you to split the original cable into up to four individual cables, with each cable using a dedicated fiber pair. Conversely, single-mode transceivers use a single pair of fiber, which prevents you from splitting the cable.

The topology on this slide shows four endpoints connected to the same FortiSwitch port using a breakout cable that splits a 40G port into four 10G ports. The 40G port on FortiSwitch uses a QSFP+ transceiver, and the port on the endpoints uses an SFP+ transceiver.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can enable split port on supported ports by running the FortiSwitchOS CLI commands shown on this slide. Note that FortiSwitch requires a reboot in order to apply the changes.

In some FortiSwitch models, the first step to configure split port is to select a port configuration layout for split port. Because of limitations on the maximum number of interfaces on the switch, some FortiSwitch requires that you select which ports to disable in favor of supporting split port on other ports. For example, on a FortiSwitch 548D model, you have the following two port configuration layout options:

1. Disable port54 so you can enable split port on port53 only.
2. Disable port41 to port48 so you can enable split port on both port53 and port54.

After you select the right layout, the FortiSwitch CLI allows you to enable split port on the corresponding ports. For models that don't require you to disable a port, you can enable split port right away. Refer to the *FortiSwitchOS—Administration Guide* and the *FortiSwitch-Managed by FortiGate* documents on `docs.fortinet.com` to know which FortiSwitch models require you to disable ports for enabling split port.

To prevent configuration loss, it is *highly* recommended that you configure split port as the first step in your setup, *before* you make any other configuration changes on FortiSwitch, or *before* you authorize FortiSwitch on FortiGate. The reason is that FortiSwitch changes the list of switch ports available on the device. In case FortiSwitch is managed on FortiGate, you must remove FortiSwitch from FortiGate first, then enable split port on FortiSwitch, and then authorize FortiSwitch again on FortiGate.

The name of each split port follows a <parent_port>.X notation. This slide shows the ports changes on a FortiSwitch 548D model when you convert port53, which is a 40G port, to four 10G ports. Note that the port configuration layout selected disables port54 from the configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about split port is true?

✓A. It is recommended to be enabled before making any other configuration changes.

B. It is supported by all FortiSwitch models and ports.

2. What is the result of selecting a port configuration layout for split port?

A. Determines the name notation to use for split ports.

✓B. FortiSwitch disables one or more ports in favor of supporting split port on other ports.

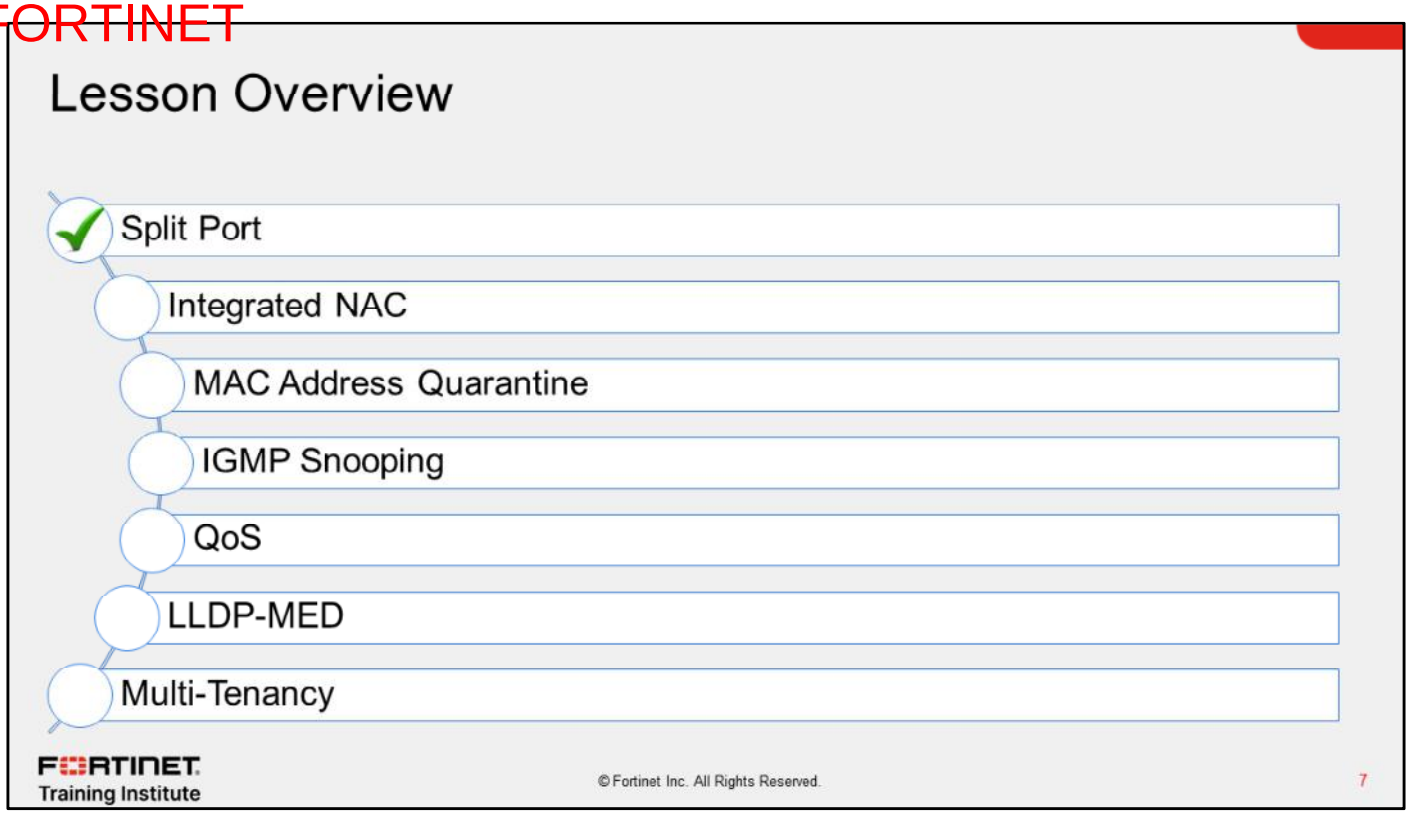
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

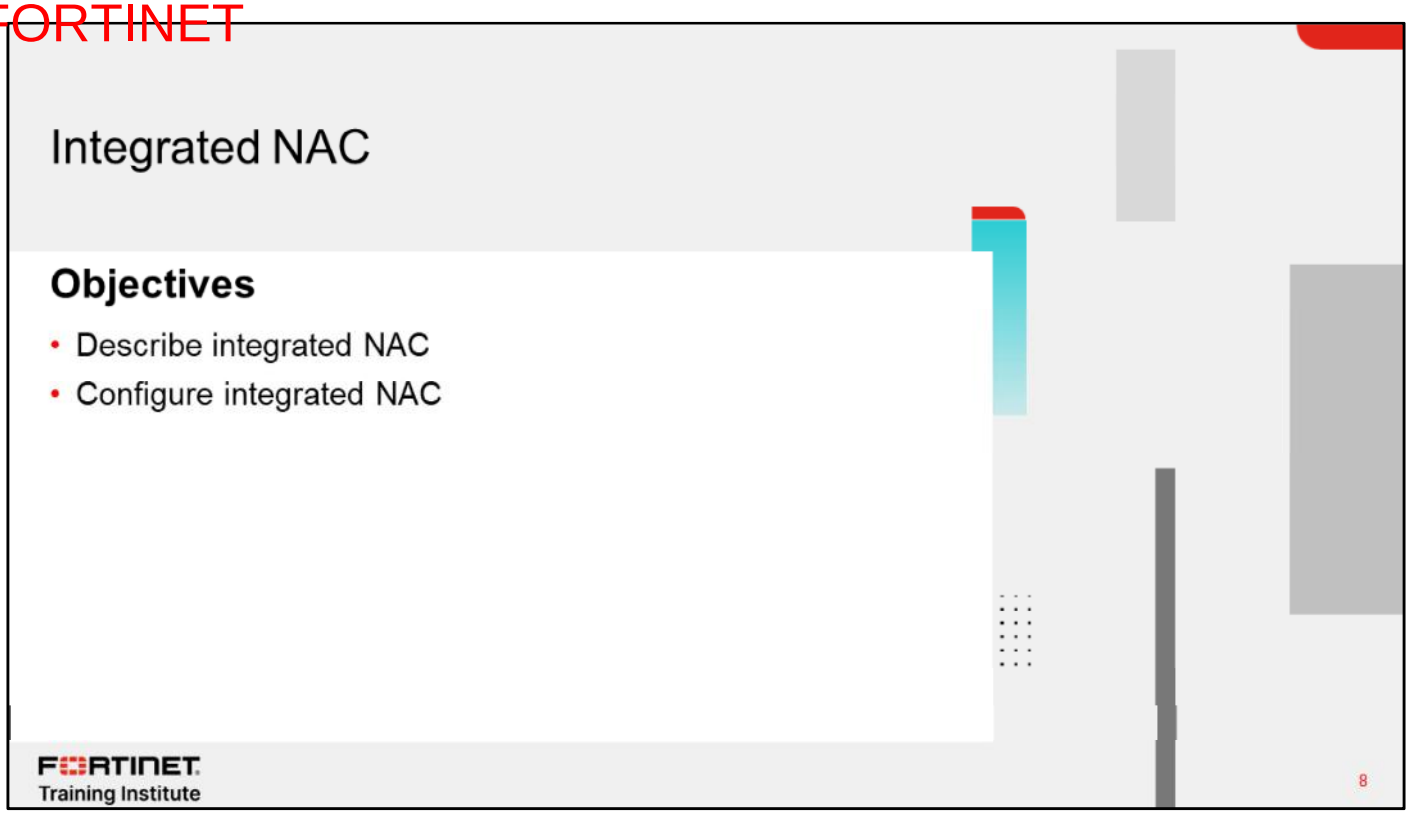


Good job! You now understand split port.

Now, you will learn about integrated NAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

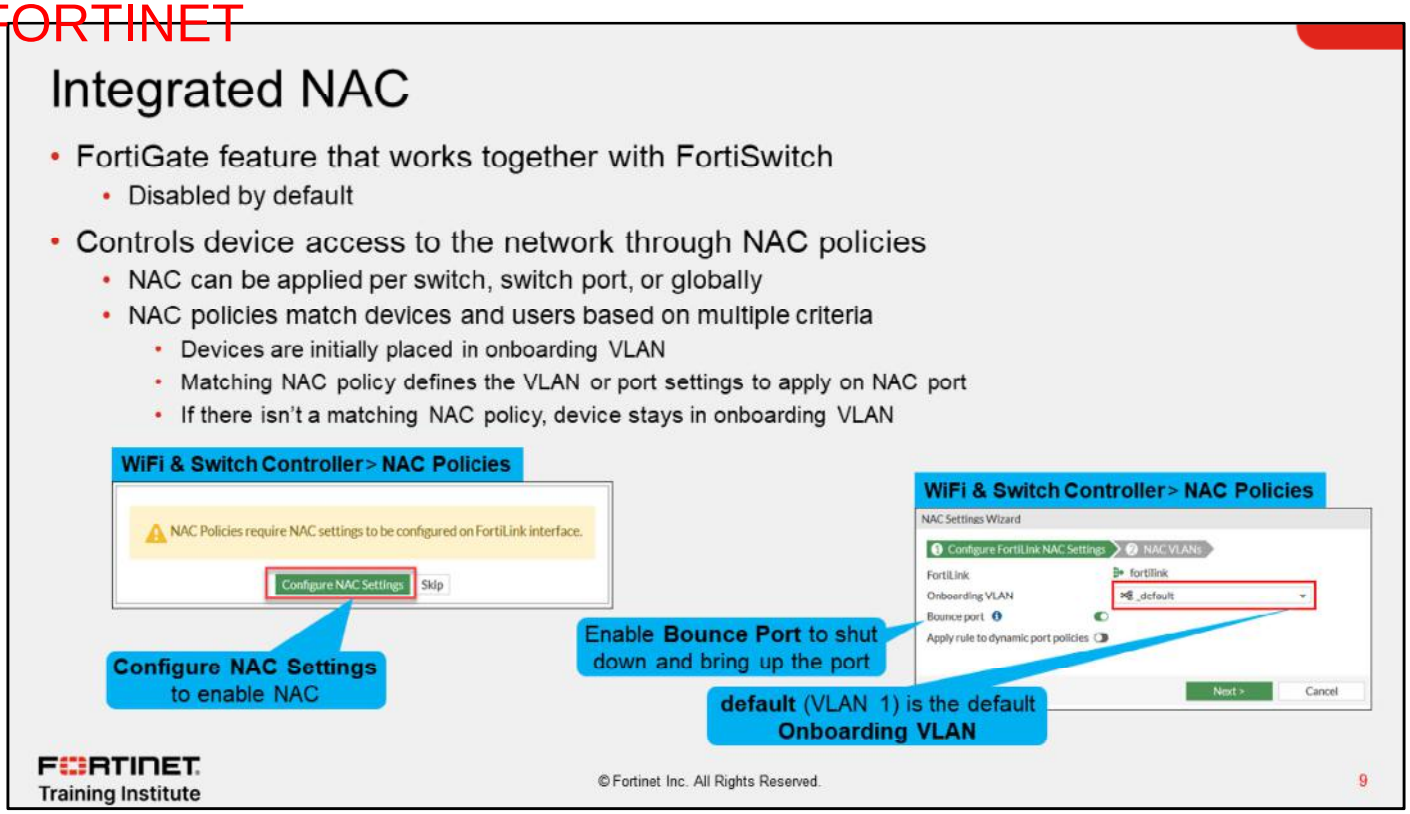


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in integrated NAC, you should be able to understand how FortiGate and FortiSwitch work together to provide network access to endpoints based on the user or device type detected by FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



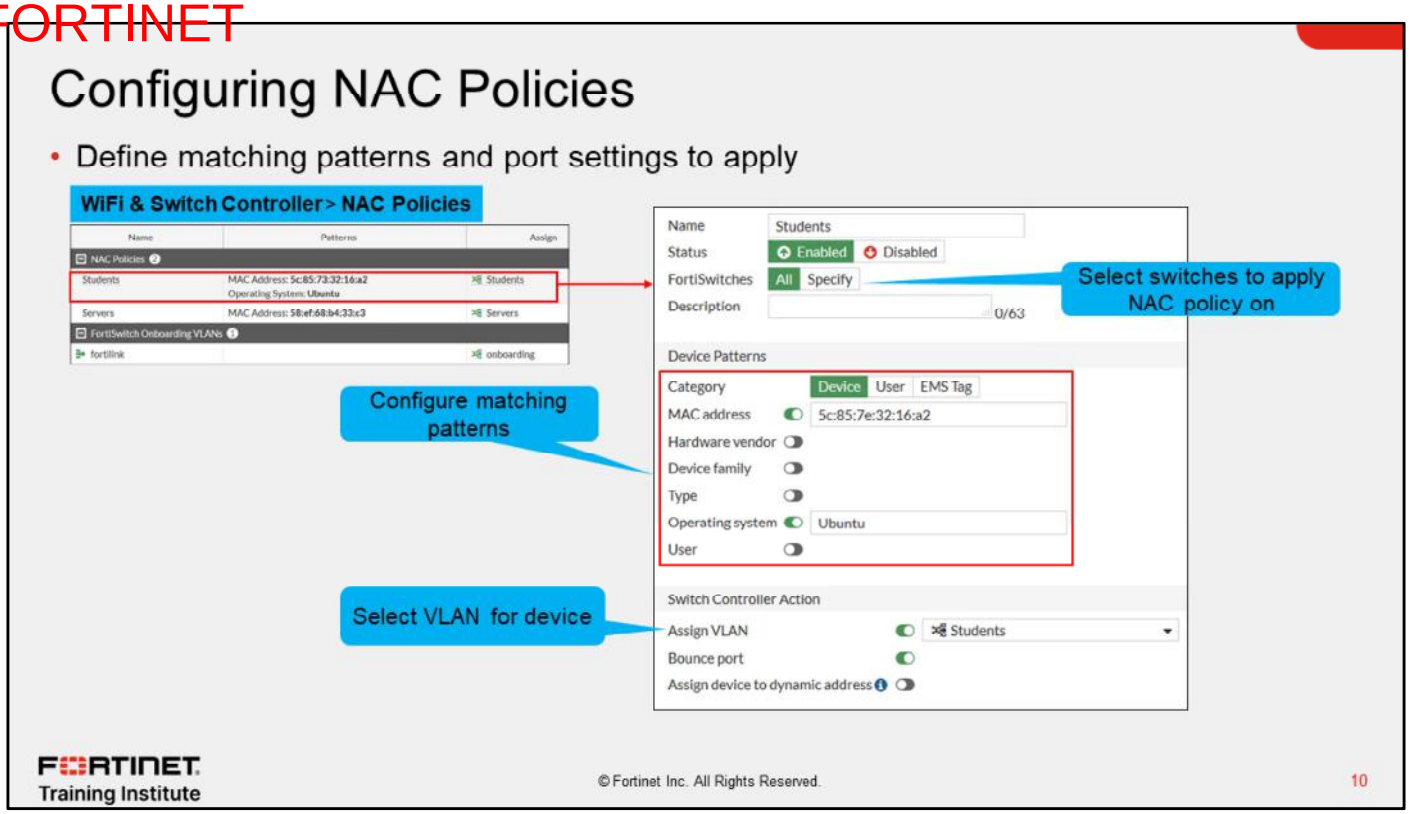
Integrated network access control (NAC) is mainly a FortiGate feature, but it requires FortiSwitch to work. It enables a managed FortiSwitch to assign a VLAN or some specific settings to the port that connects a device, based on the matching NAC policy detected by FortiGate for a device. You configure NAC policies on FortiGate that define the matching criteria (or patterns), as well as the settings to apply on the corresponding switch port when the NAC policy matches.

Integrated NAC is disabled by default. To enable the feature, access the **NAC Policies** menu on the FortiGate GUI. After that, you need to follow the wizard to configure basic NAC settings, such as selecting the onboarding VLAN for NAC. By default, the onboarding VLAN is **default**, which is assigned with the VLAN ID 1. However, you can select any of the existing FortiSwitch VLANs if required. The onboarding VLAN is always assigned as the native VLAN on a port that is subject to NAC. As a result, the traffic for the device connected on the port is placed on the onboarding VLAN initially. After the device or user is identified, FortiGate applies the VLAN or port settings configured in the matching NAC policy. If there are no matching NAC policies, the device stays in the onboarding VLAN.

After the VLAN or port settings are applied on the port, you may want to shut down and bring up the port to restart the DHCP process on the device, because the device may have been moved to a different VLAN with different DHCP settings. To have FortiGate automatically bounce the port after detection, enable **Bounce Port** on the FortiLink NAC Settings wizard.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A NAC policy indicates the device type, user, or EMS tag that FortiGate checks on a device, and if there is a match, the VLAN or settings to apply on the FortiSwitch port. Like firewall policies, NAC policies are checked from top to bottom until a policy that matches *all* the defined patterns is found.

When you configure a NAC policy, you can select if you want the policy to apply to all managed switches or specific ones. Note that the list of switches selected on a NAC policy takes precedence over the list of switches selected on the FortiLink interface.

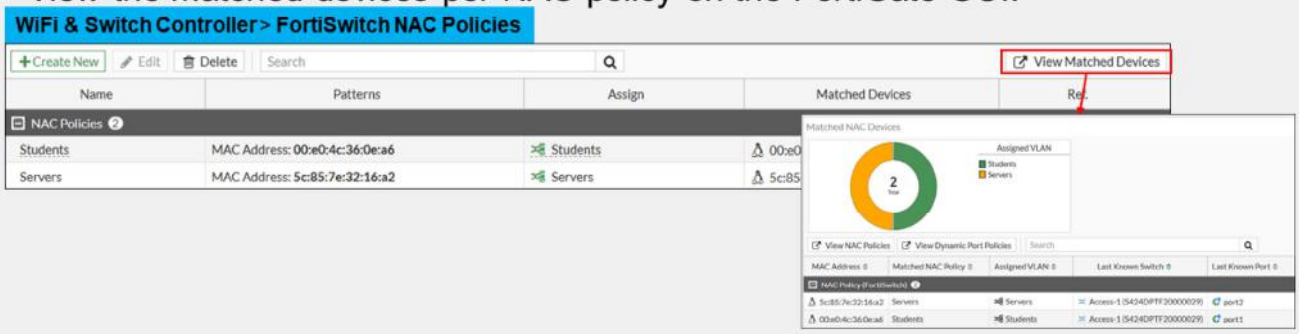
When there is a matching NAC policy, FortiGate assigns the port to the VLAN selected in the **VLAN** drop-down list. Additionally, you can configure the NAC policy to bounce the port when it is the matching policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Viewing Matched Devices

- View the matched devices per NAC policy on the FortiGate GUI:



- View the matched devices per NAC policy on the FortiGate CLI:

```
# diagnose switch-controller mac-device nac known
Vdom: root
MAC                LAST-KNOWN-SWITCH  LAST-KNOWN-PORT    MATCHED-NAC-POLICY MAC-POLICY-ACTION  LAST-SEEN  FSW-ID
COMMENTS
00:e0:4c:36:0e:a6  S424DPTF20000029   port1              Students           Students           0          3
5c:85:7e:32:16:a2  S424DPTF20000029   port2              Servers            Servers            664        2
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

You can see the list of matched devices on the FortiGate GUI and CLI. Note that if the device hostname has been detected by FortiGate, the GUI displays the device hostname instead of its MAC address. The CLI output, however, always displays the device MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about integrated NAC is true?
   A. It is enabled by default.
   ✓B. FortiGate applies configured settings on the FortiSwitch port based on matching NAC policy.

2. What is the **Onboarding VLAN** setting used for in integrated NAC?
   ✓A. Devices without a matching NAC policy are placed in the selected onboarding VLAN.
   B. Devices with a matching NAC policy are placed in the selected onboarding VLAN.

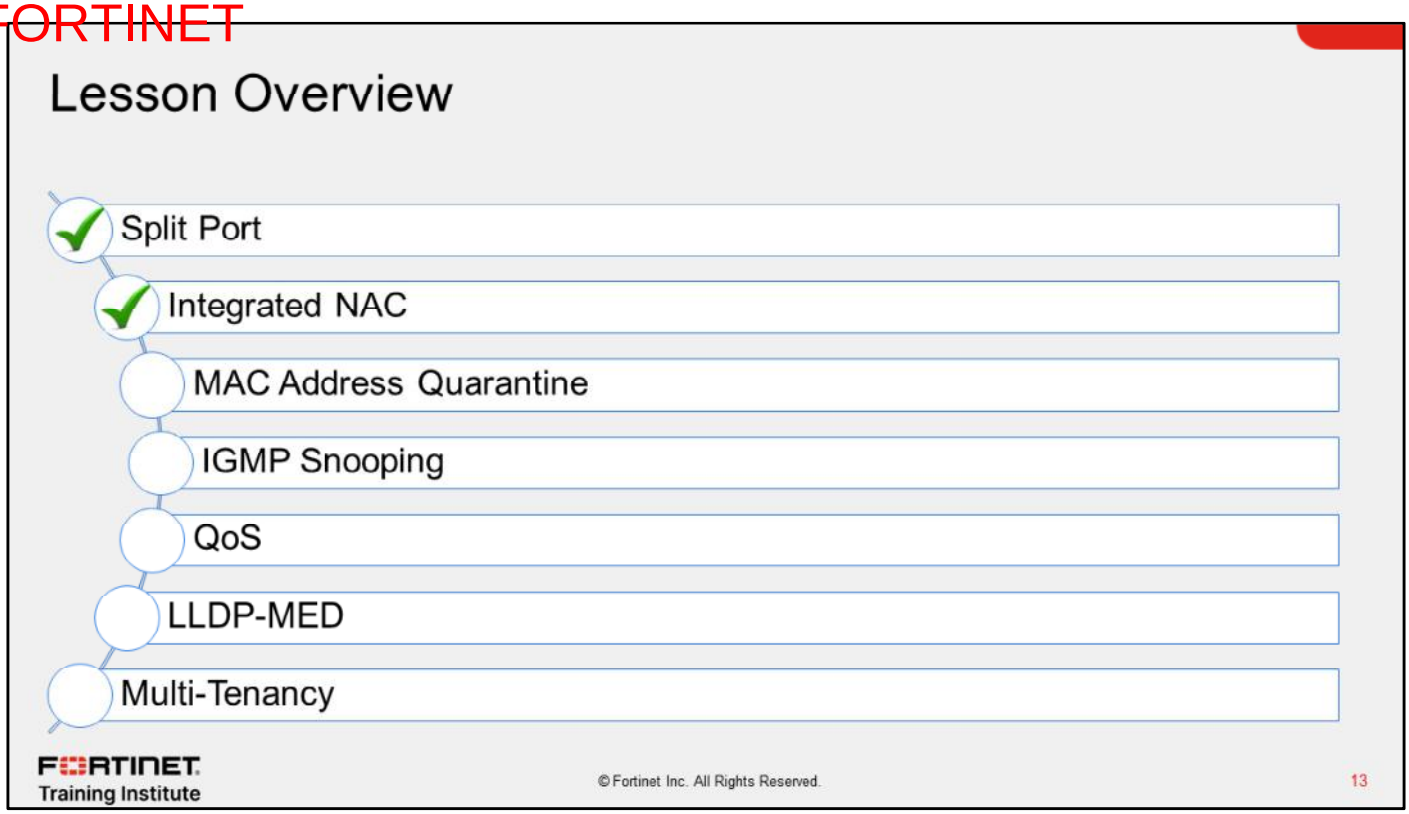
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

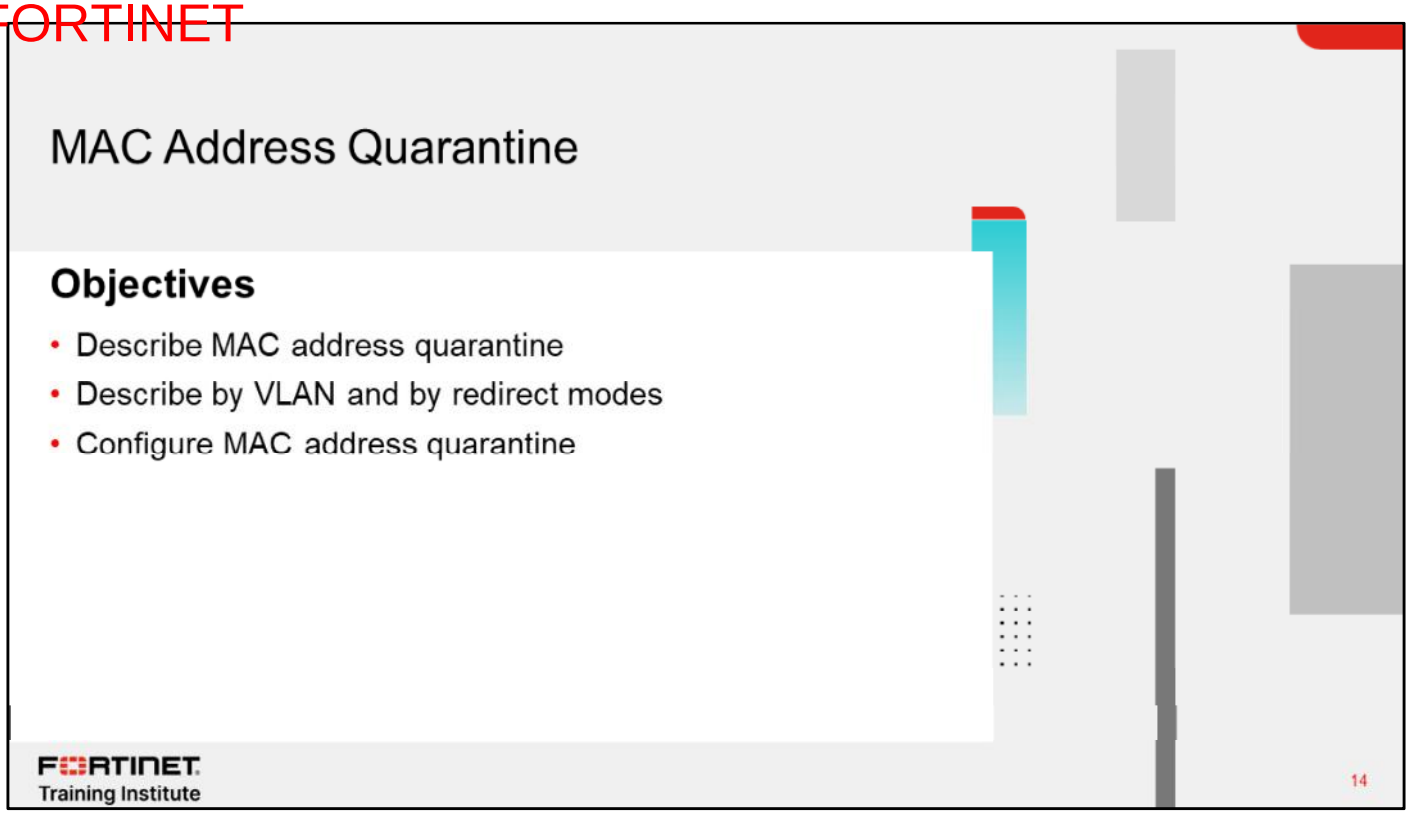


Good job! You now understand integrated NAC.

Now, you will learn about MAC address quarantine.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

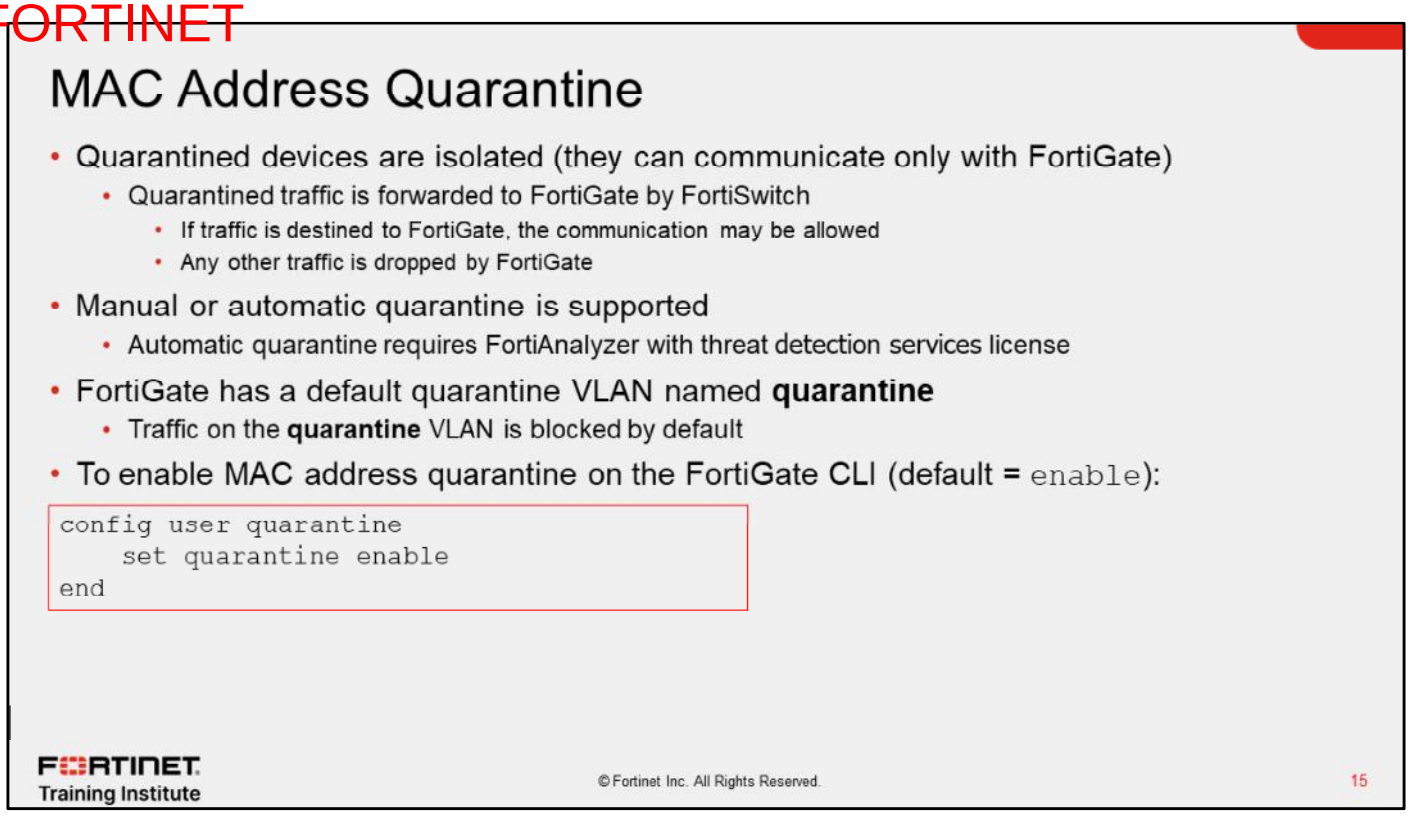


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in MAC address quarantine, you should be able to understand how to automatically or manually quarantine devices at Layer 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



For quarantining a MAC address, FortiSwitch and FortiGate work together to isolate a device. Isolation means that a quarantined device can communicate only with FortiGate. If the device tries to communicate with any other host in the network, the communication is blocked. To isolate a quarantined device, FortiSwitch forwards all its traffic to FortiGate. The traffic can be any of the following destinations:

- FortiGate local: The destination is a FortiGate interface.
- Intra-VLAN: The destination is a device in the same VLAN.
- Inter-VLAN: The destination is a device in a different VLAN or network that is reached through FortiGate.

For the FortiGate local traffic, the communication is allowed if FortiGate is configured to allow the connection. For example, a quarantined device can ping a FortiGate interface if ping access is enabled on that interface. For other traffic, the communication is blocked by FortiGate.

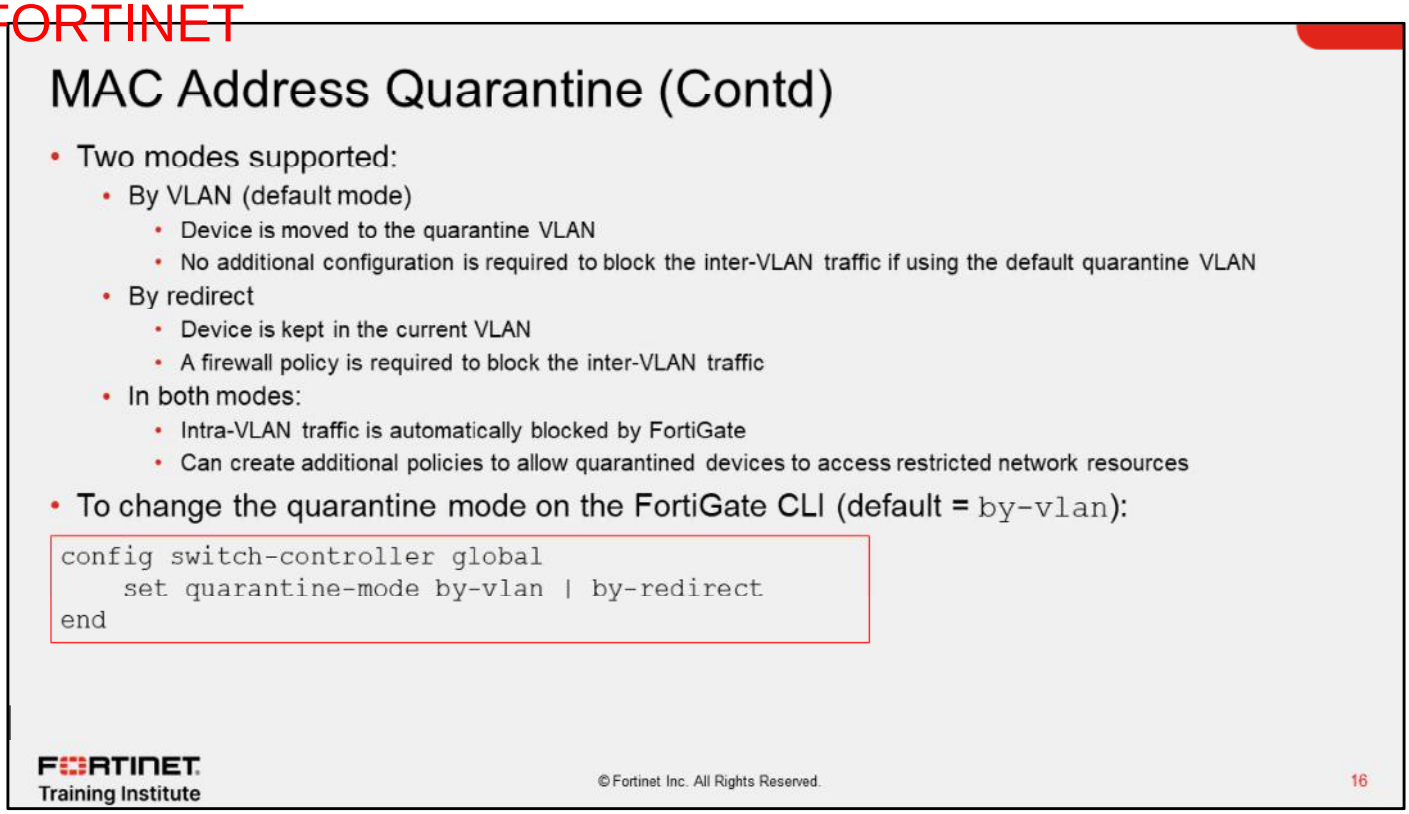
You can quarantine devices by MAC address, either manually or automatically. MAC address quarantine works as follows:

1. FortiGate monitors the device activity based on the traffic and security logs generated for the device.
2. If FortiGate determines that the device must be quarantined, either because an automated rule has been triggered, or because of user intervention, FortiGate adds the device MAC to its local quarantine list.
3. FortiGate applies the quarantine-related configuration for the quarantined device to FortiSwitch using the FortiSwitch REST API.
4. The pushed configuration instructs FortiSwitch to block the traffic from the quarantined MAC address.

Note that automatic quarantine requires a FortiAnalyzer device with a valid threat detection services license. To enable MAC address quarantine on the FortiGate CLI, run the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate supports two MAC address quarantine modes: by VLAN and by redirect. In both modes, FortiGate blocks the traffic from the quarantined MAC address, provided the correct configuration is in place.

In by VLAN mode, which is the default mode, FortiGate moves the quarantined MAC address to the quarantine VLAN. If you are using the default **quarantine** VLAN as your quarantine VLAN, the inter-VLAN traffic from the device is automatically blocked because the **quarantine** VLAN does not have any firewall policies configured. Note that the device can still get an IP address through DHCP because the **quarantine** VLAN has the DHCP server enabled by default.

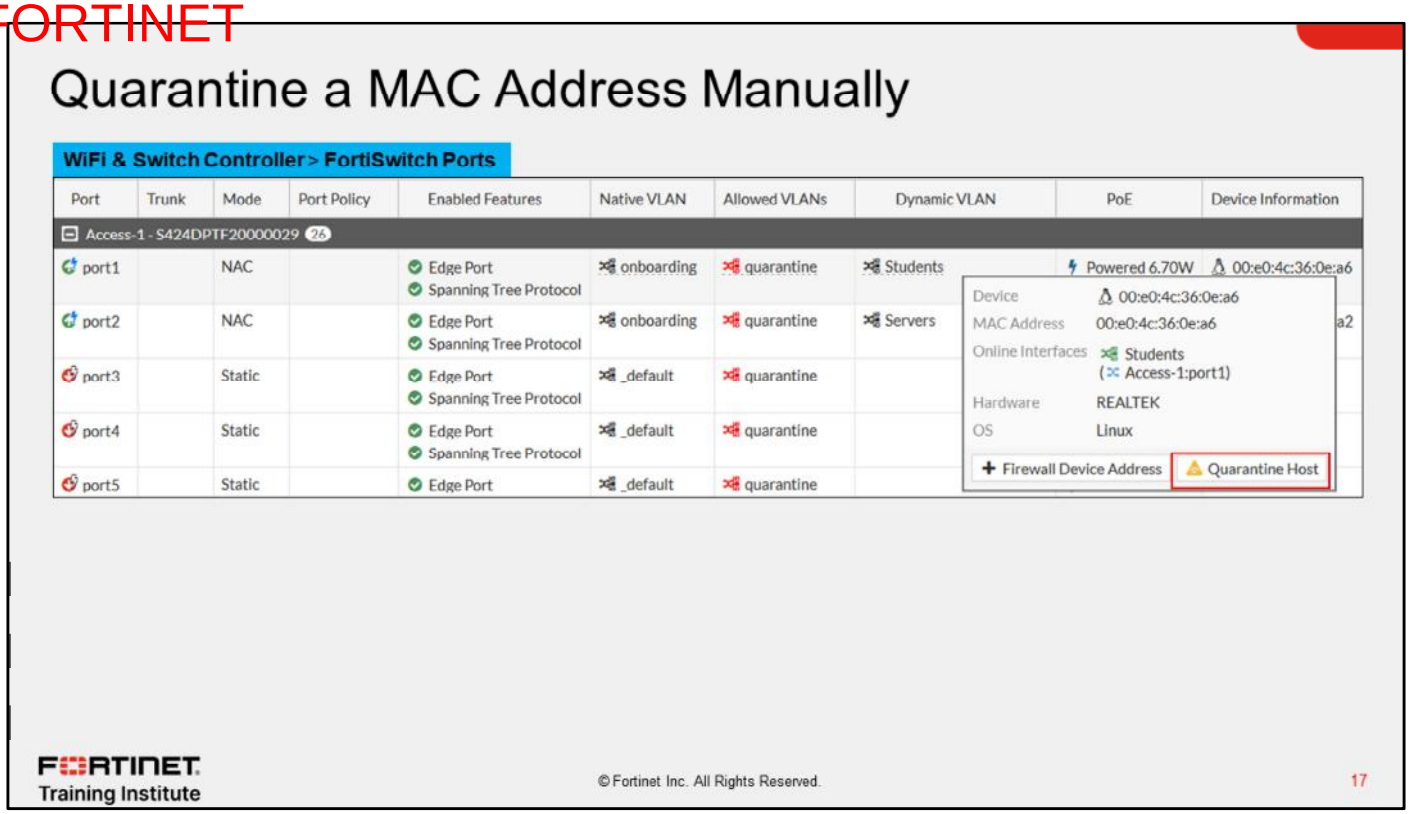
In by redirect mode, FortiGate keeps the device in its current VLAN, and adds the device MAC address to the **QuarantinedDevices** firewall address group. The device IP address does not change, which is useful for performing remediation. However, to block the inter-VLAN traffic, you must configure a firewall policy to explicitly block the traffic from the **QuarantinedDevices** address group.

In both modes, the intra-VLAN traffic is automatically dropped by FortiGate because the destination MAC address of the traffic does not match the FortiGate interface. The destination MAC address of the traffic is the MAC address of the target device located in the same VLAN. In addition, communication between the quarantined devices and FortiGate is allowed. You can also configure additional firewall policies to explicitly allow quarantined devices to access limited network resources, such as servers with Windows updates and other security-related software updates, which are required for remediation.

To change the MAC address quarantine mode on the FortiGate CLI, run the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To manually quarantine a MAC address on the FortiGate GUI, browse to the **FortiSwitch Ports** page, hover over the device listed in the **Device Information** column, and then select **Quarantine Host**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about MAC address quarantine is true?
   A. By VLAN mode is the default mode.
   ✓B. Automatic quarantine requires a FortiAnalyzer device with a valid threat services license.

2. Which statement about quarantine by redirect mode is true?
   A. Quarantined device is moved to the VLAN selected as quarantine VLAN.
   ✓B. Quarantined device stays in the same VLAN.

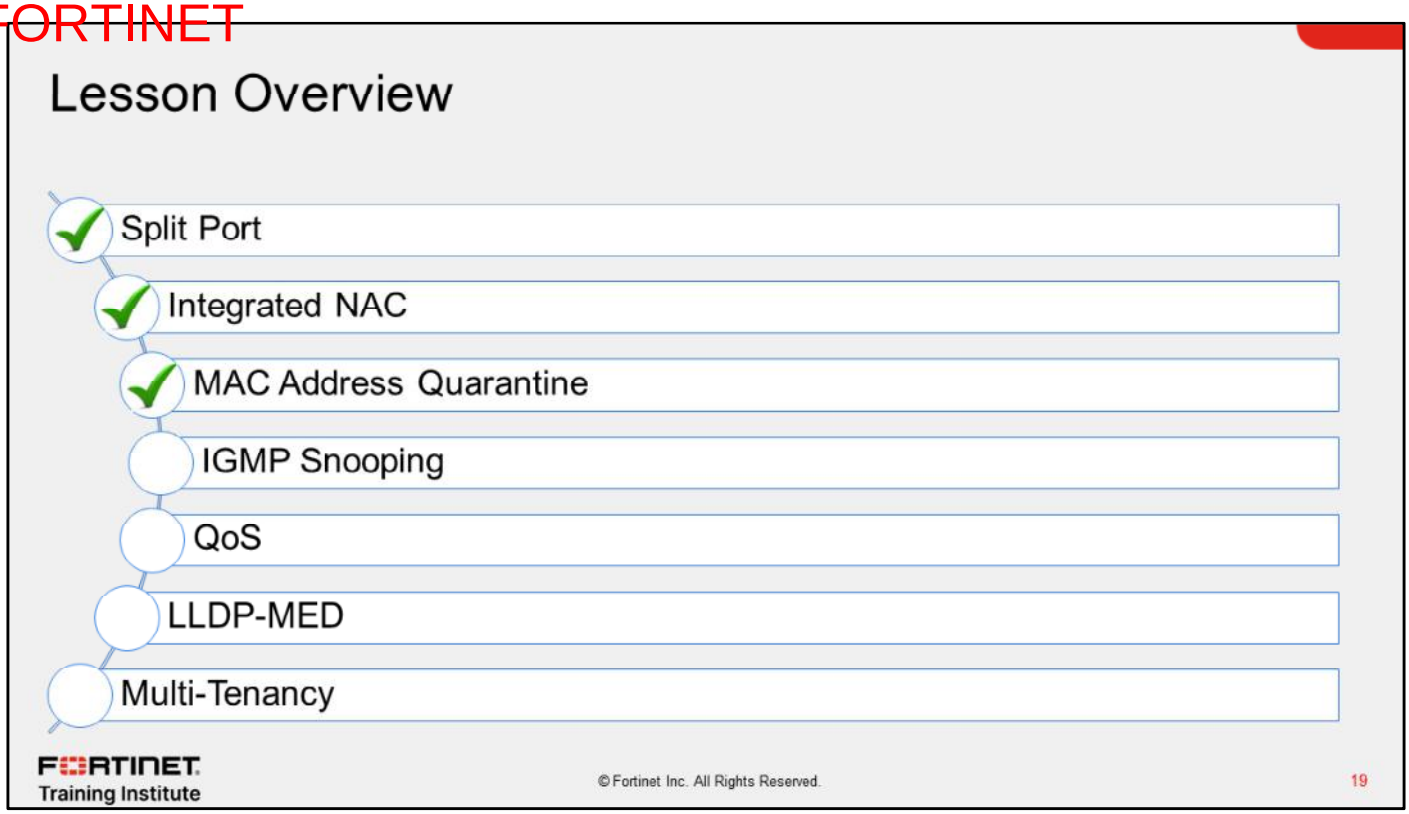
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

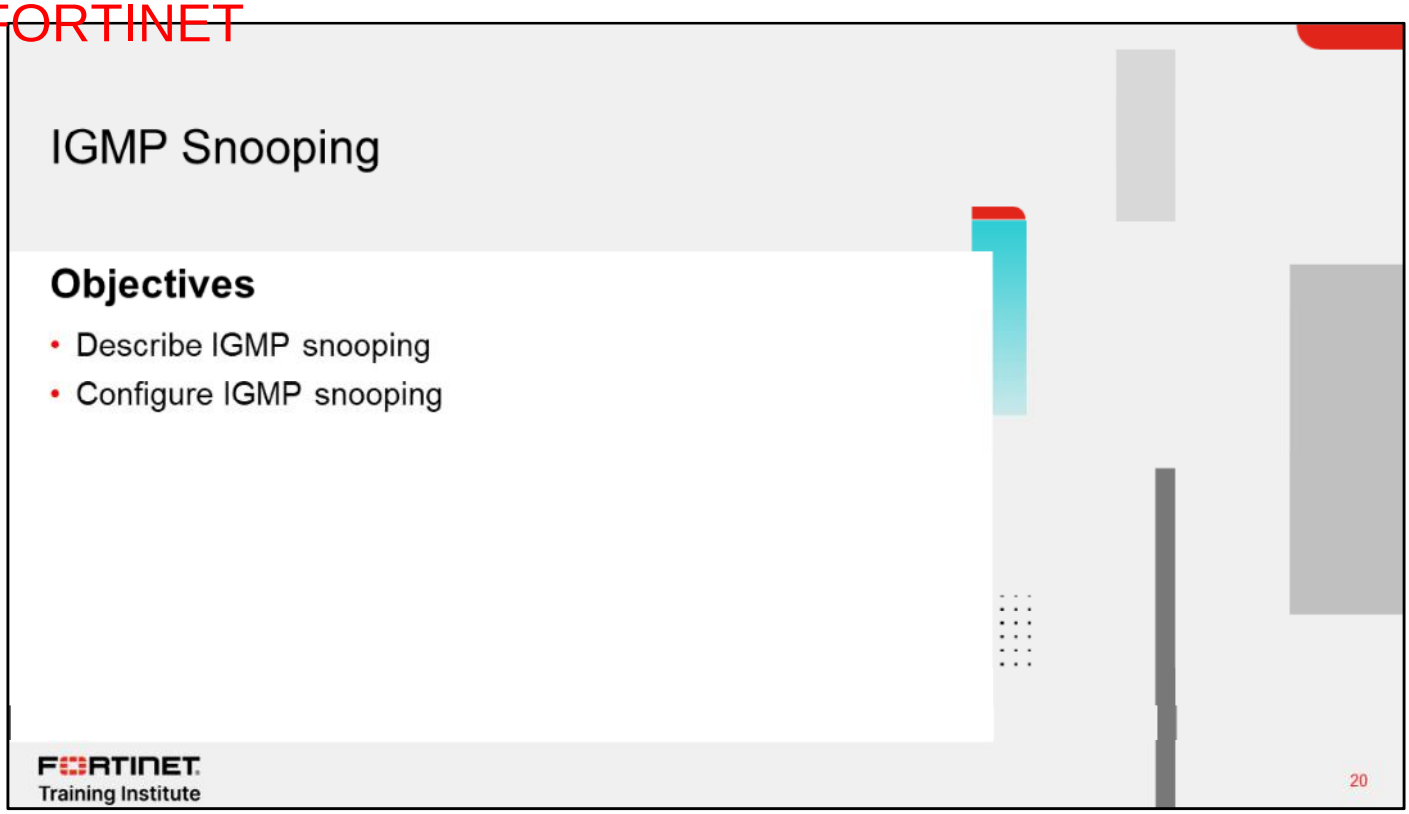


Good job! You now understand MAC address quarantine.

Now, you will learn about IGMP snooping.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

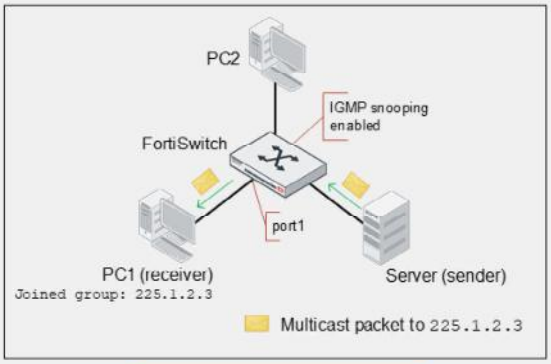
By demonstrating competence in IGMP snooping, you should be able to understand how FortiSwitch can efficiently transmit multicast traffic by inspecting IGMP messages sent by connected multicast receivers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IGMP Snooping

- Listens to IGMP report messages to:
  - Identify active multicast receivers
    - Reduces unnecessary multicast traffic in the network
    - Prevents data leaks
- Maintains multicast Layer 2 forwarding table
  - Entry added upon IGMP report join message
  - Entry removed upon IGMP report leave message
  - Multicast traffic is forwarded to active receivers only
- IGMP versions supported:
  - v1 and v2: fully supported
  - v3: no support for source filtering
    - Multicast groups and traffic handled like IGMPv2



Multicast Layer 2 Forwarding Table		
port	VLAN	Multicast Group
port1	10	225.1.2.3

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

By default, FortiSwitch treats multicast in the same way as broadcast. That is, multicast frames are flooded to all switch ports regardless of whether the connected devices need to receive the traffic. If your network has devices that run multicast applications that transmit considerable amounts of data, such as audio or video, flooding the traffic to all ports can result in potential performance issues, as well as data leaks.

IGMP snooping enables FortiSwitch to forward multicast traffic only to ports that connect to active multicast receivers. When a device is interested in receiving multicast traffic, it sends an IGMP report join message that indicates the multicast group it wants to join. FortiSwitch passively listens to IGMP report join messages received at ports to discover multicast receivers. FortiSwitch then uses this information to populate its multicast Layer 2 forwarding table with the multicast groups discovered on each port. The result is that when FortiSwitch receives traffic from a sender that is destined to a particular multicast group, FortiSwitch forwards the traffic only to matching ports, thus reducing unnecessary multicast traffic in the network. Moreover, when a device wants to stop receiving multicast traffic, it sends an IGMP report leave message. FortiSwitch then removes the corresponding entry from the multicast Layer 2 forwarding table.

FortiSwitch supports IGMP versions 1 and 2 fully, and version 3 partially. For version 3, FortiSwitch doesn't support source filtering, which is a feature that enables you to define specific source addresses that a receiver wants to receive multicast traffic from. When FortiSwitch processes IGMPv3 messages, it creates multicast groups and forwards traffic based on the same way it does for IGMPv2.

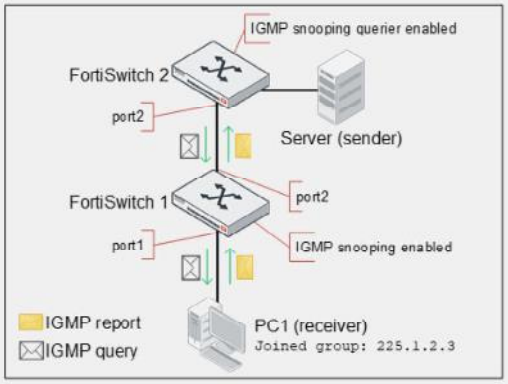
The topology on this slide shows three endpoints connected to FortiSwitch. All endpoints are placed in the same VLAN: VLAN 10. PC1, which is connected to port1 on FortiSwitch, has joined the multicast group `225.1.2.3`. Because FortiSwitch has IGMP snooping enabled, FortiSwitch forwards the multicast traffic destined to `225.1.2.3`, and sent by the server, to port1 only. If IGMP snooping were disabled, then PC2 would have also received a copy of the multicast traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IGMP Snooping Querier and MRouter Port

- When IGMP snooping is enabled:
  - FortiSwitch doesn't forward IGMP reports to ports except mRouter ports
    - Adjacent switches can't discover non-directly connected receivers
- Enable IGMP snooping querier to:
  - Get immediate IGMP reports received by other switches
  - Send periodic IGMP queries on a VLAN to get IGMP reports to prevent active receivers from aging
- mRouter ports:
  - Port where IGMP query is received
  - IGMP reports are forwarded to mRouter ports only
    - Multicast traffic is also forwarded to mRouter ports



FortiSwitch 1—Multicast Layer 2 Forwarding Table

port	VLAN	Multicast Group
port1	10	225.1.2.3
port2	10	querier

FortiSwitch 2—Multicast Layer 2 Forwarding Table

port	VLAN	Multicast Group
port2	10	225.1.2.3

MRouter port (querier)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

When you enable IGMP snooping, FortiSwitch listens to incoming IGMP report messages but doesn't forward them to any port except mRouter ports. This behavior prevents switches from discovering multicast receivers that aren't directly connected. As a result, receivers are unable to get multicast traffic from senders connected to other switches. In addition, multicast receivers send IGMP report join messages only when they join a group, and don't send more IGMP report join messages unless they get an IGMP query requesting their status. This means that, if there are no IGMP queriers, the entries for multicast receivers in the multicast Layer 2 forwarding table eventually age despite still being active.

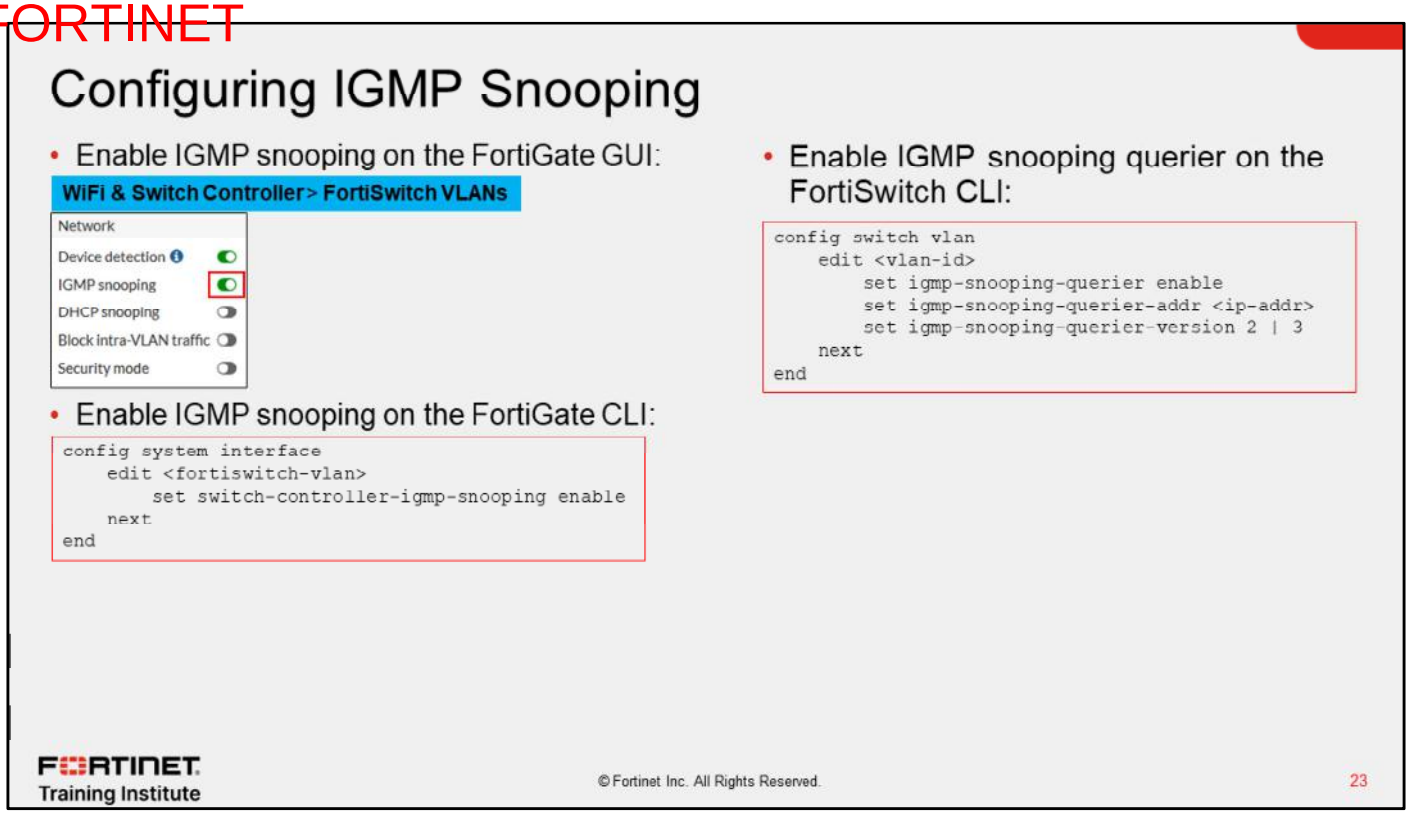
To solve the previous two issues, you can enable IGMP snooping querier on FortiSwitch to instruct the switch to send periodic IGMP query messages on a VLAN to get IGMP membership reports from receivers on that VLAN. The goal is to keep the information on multicast Layer 2 forwarding tables consistent across switches, thus preventing multicast traffic loss. You can enable IGMP snooping querier on multiple switches on a per-VLAN basis. However, if FortiSwitch detects a query message from another device with a lower IP address, it stops sending queries for a specific amount of time.

When FortiSwitch receives an IGMP query from a neighbor, it flags the receiving port as an mRouter port. In addition to forwarding multicast traffic, FortiSwitch also forwards IGMP reports to all its mRouter ports, enabling IGMP queriers to get immediate updates about receivers that join or leave multicast groups.

The topology on this slide shows two endpoints in VLAN 10, each connected to a different switch. PC1, which is connected to port1 on FortiSwitch 1, has joined the multicast group `225.1.2.3`. Because FortiSwitch 2 has IGMP snooping querier enabled, FortiSwitch 1 forwards IGMP reports sent by PC1 to FortiSwitch 2 through port2. This enables FortiSwitch 2 to become aware of receivers that are not directly connected to the switch. FortiSwitch 2 also sends periodic IGMP queries on VLAN 10 to get the IGMP membership reports from receivers, and consequently prevents their entries in the forwarding table from aging.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

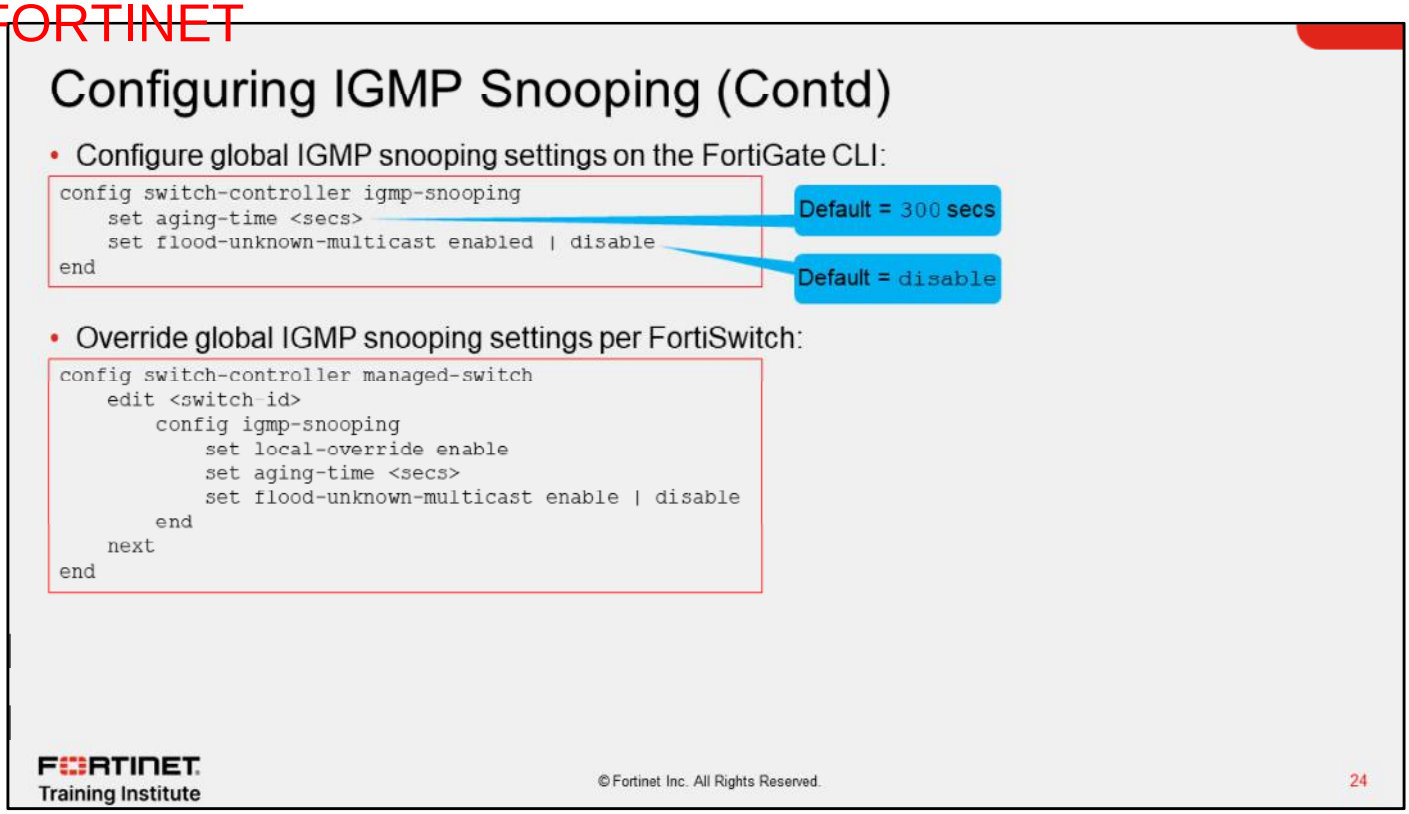


IGMP snooping is disabled by default. This slide shows how to enable IGMP snooping on a VLAN using the FortiGate GUI and CLI.

If you also want to enable IGMP snooping querier, you must do so on the FortiSwitch CLI directly, as shown on this slide. For the IGMP snooping querier feature, you can also select the source IP address of the query—`0.0.0.0` by default—as well as the IGMP version to use—version `2` by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



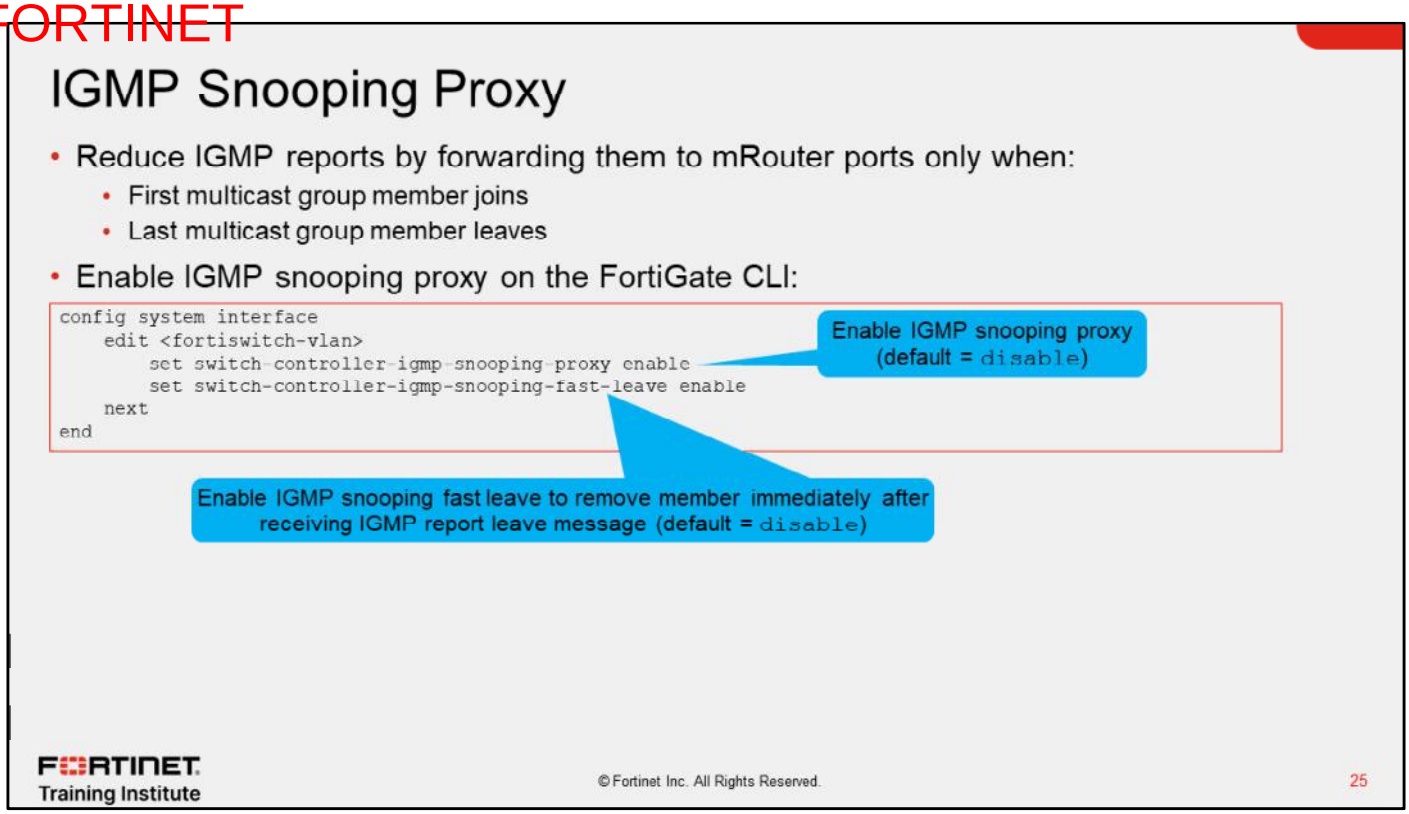
This slide shows how to configure the global IGMP snooping settings using the FortiGate CLI, and how to override them per switch.

By default, dynamic entries in the multicast Layer 2 forwarding table expire after 300 seconds of receiving the last IGMP report join message, an aging period that works for most deployments. You can still change the aging period by adjusting the `aging-time` setting.

In addition, when you enable IGMP snooping, FortiSwitch drops unknown multicast traffic by default. Unknown multicast traffic refers to multicast traffic destined to a multicast group address with no entry in the multicast Layer 2 forwarding table. You can change this behavior by enabling the `flood-unknown-multicast` setting as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In large networks with a very high number of multicast receivers, the number of IGMP report messages can be considerable. Because FortiSwitch forwards IGMP reports to mRouter ports, an elevated number of multicast receivers can increase the system resource usage on the IGMP querier device.

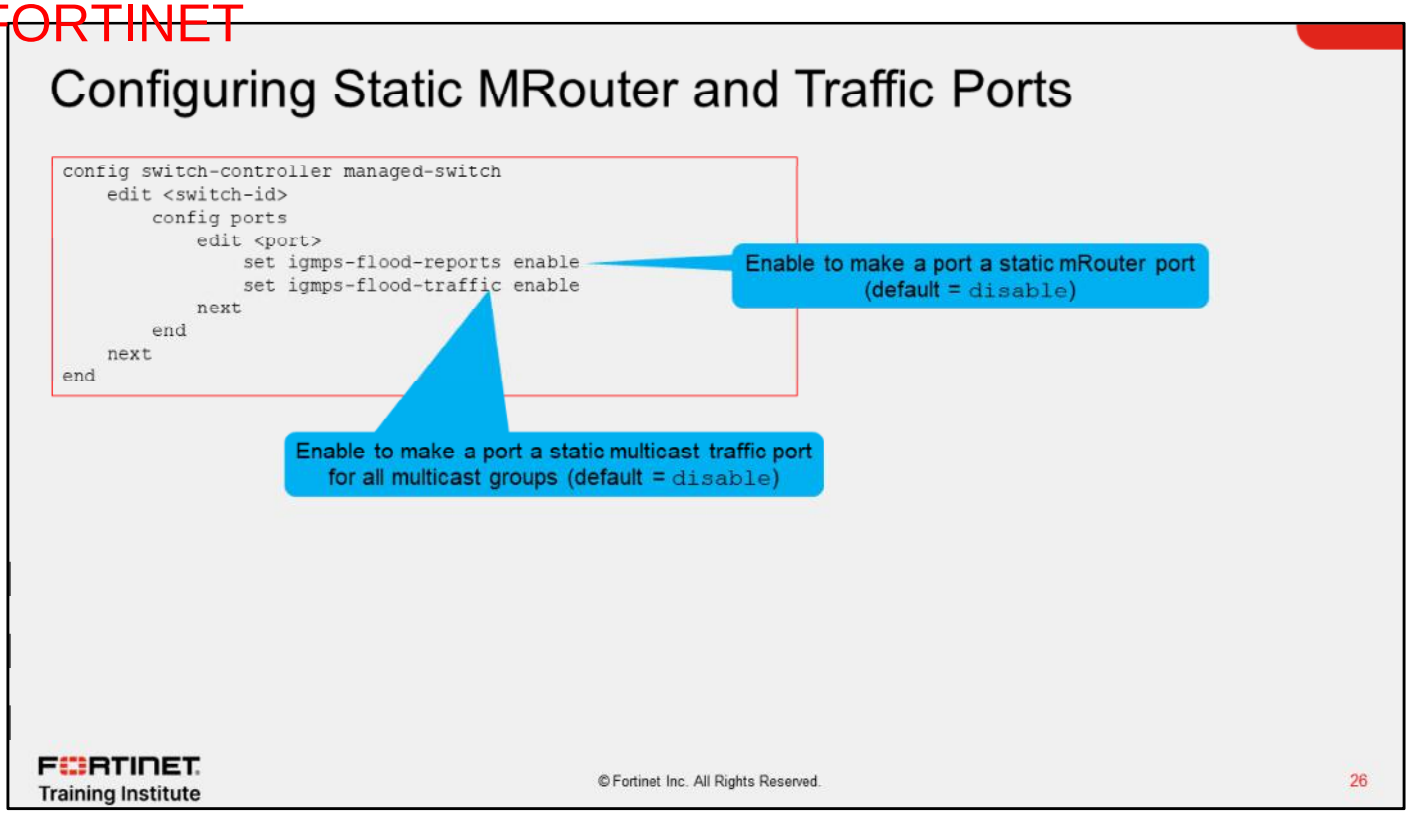
To reduce the number of IGMP reports processed by the IGMP querier, you can enable IGMP snooping proxy on FortiSwitch. When you enable IGMP snooping proxy, FortiSwitch forwards IGMP reports only when the first member of a multicast group joins and when its last member leaves.

When you enable IGMP snooping fast leave, FortiSwitch removes a member from the multicast Layer 2 forwarding table immediately after receiving an IGMP report leave message. If you enable IGMP snooping proxy, you can instruct FortiSwitch to wait for a period of time—10 seconds by default—before removing the member from the table.

This slide shows how to enable IGMP snooping proxy and IGMP snooping fast leave on a VLAN using the FortiGate CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



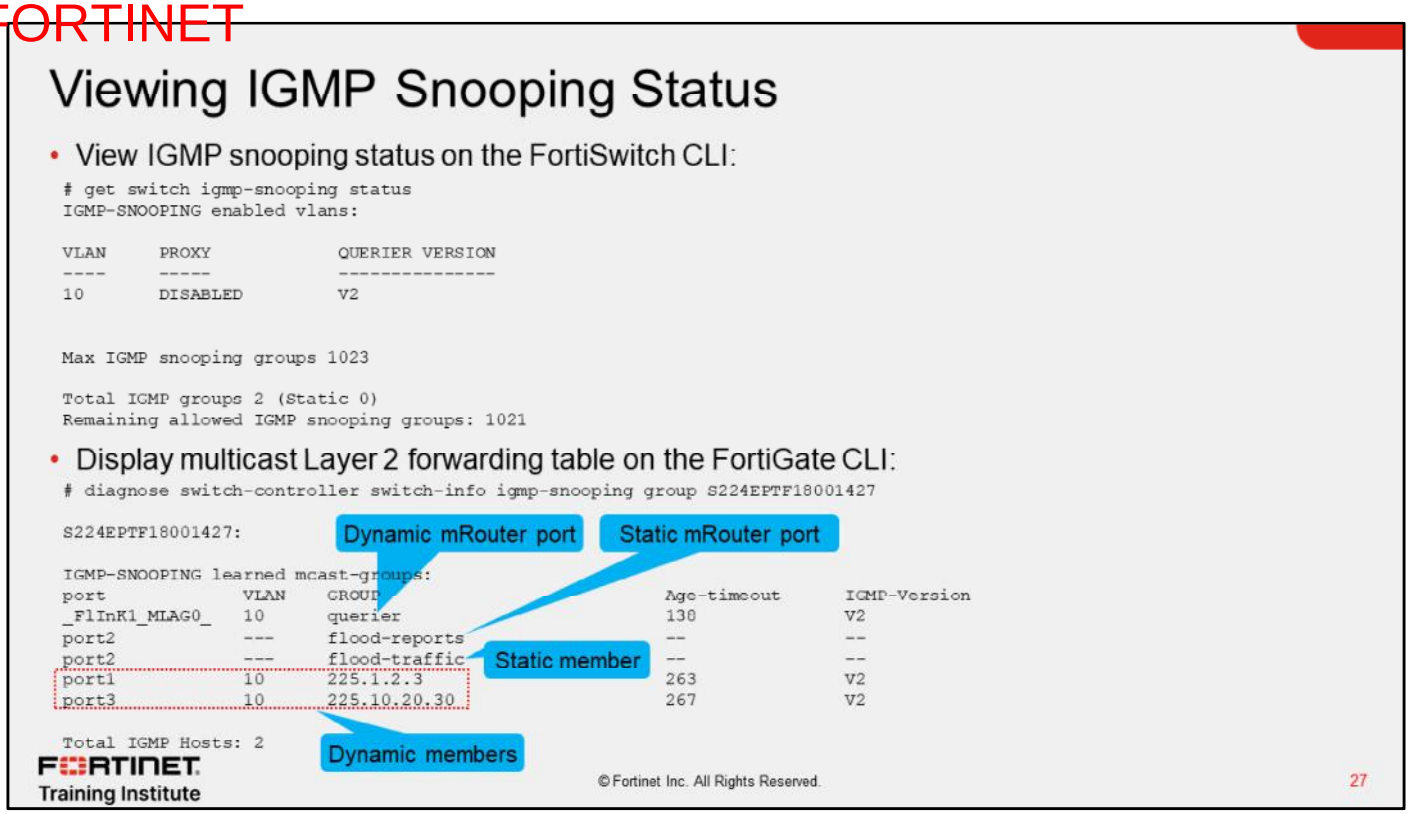
FortiSwitch dynamically flags ports receiving IGMP queries as mRouter ports. However, you can also statically make other ports mRouter ports by enabling the `igmps-flood-reports` setting on the port.

In addition, you can also instruct FortiSwitch to always forward multicast traffic to a port, regardless of the target multicast group, by enabling the `igmps-flood-traffic` setting on the port.

This slide shows how to enable such settings using the FortiGate CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to display the IGMP snooping status and groups using the FortiSwitch CLI and FortiGate CLI, respectively. The output for the IGMP groups detected by FortiSwitch includes static and dynamic multicast group members (receivers). It also shows which ports are identified as dynamic or static mRouter ports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about IGMP snooping is true?
   - A. FortiSwitch floods unknown multicast traffic by default.
   - ✓ B. Reduces unnecessary multicast traffic and prevents data leaks.

2. What is the default aging time for dynamic entries in the multicast Layer 2 forwarding table?
   - A. 30 seconds
   - ✓ B. 300 seconds

3. Which statement about mRouter ports is true?
   - A. A port must be manually configured as mRouter by the administrator.
   - ✓ B. A port automatically becomes an mRouter port after receiving an IGMP query.

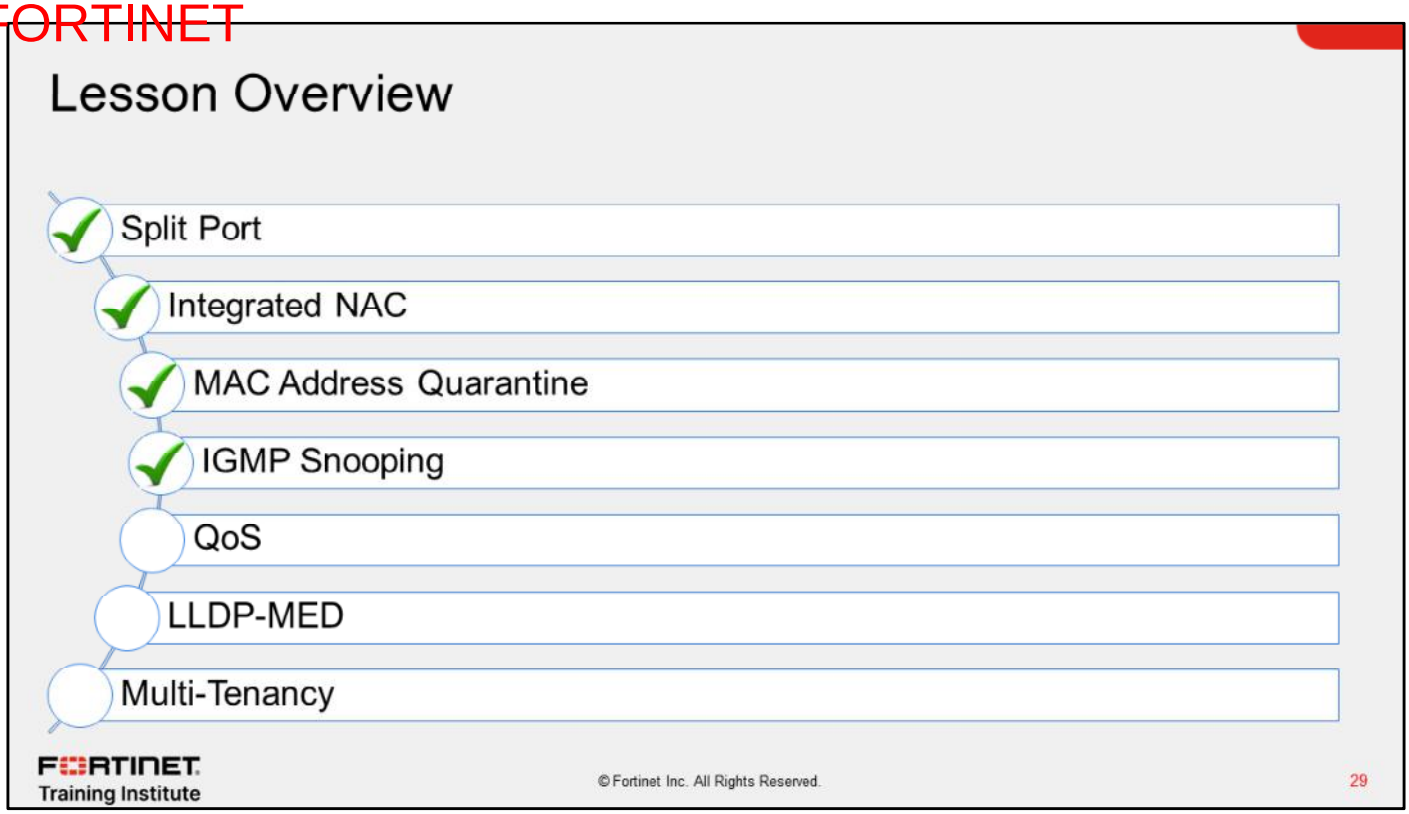
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

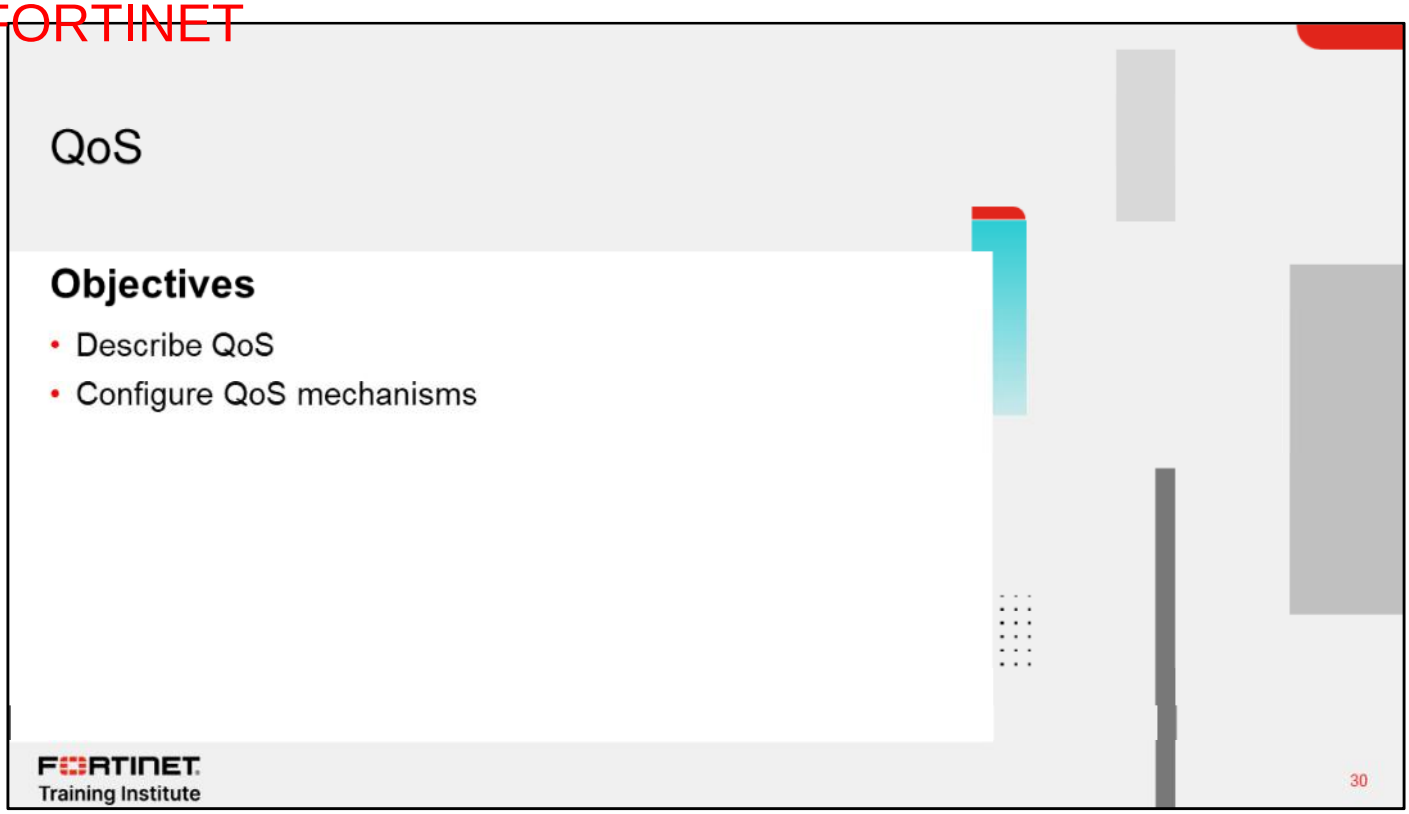


Good job! You now understand IGMP snooping.

Now, you will learn about QoS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

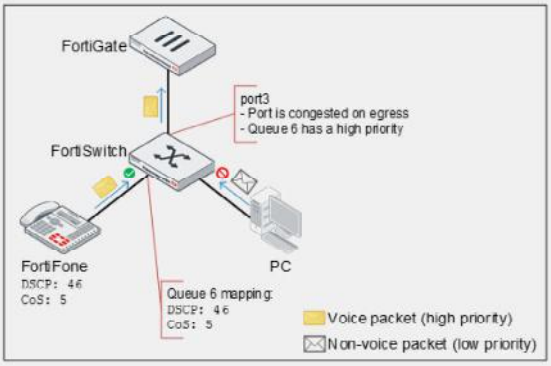
By demonstrating competence in QoS, you should be able to understand the different QoS mechanisms supported by FortiSwitch to ensure critical traffic is prioritized.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

QoS

- Mechanisms that identify and prioritize traffic
  - Critical and sensitive applications are expedited during network congestion
    - Common use case: voice and video
- FortiSwitch supports QoS through:
  - Ingress traffic:
    - Marking
      - Existing CoS and DSCP markings in packets are kept (trusted) or remarked using ACLs
    - Classification
      - Packets with matching CoS or DSCP markings are mapped to an egress queue (8 queues per port)
  - Egress traffic:
    - Queuing
      - Packets are processed based on scheduling and queue priority
      - During severe congestion on egress port, packets may be dropped based on drop policy set on queue
    - Rate limiting
      - Packets exceeding maximum rate set on queue are dropped
      - Packets below minimum rate set on queue aren't dropped



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

QoS refers to the use of mechanisms that enable network devices to identify and prioritize traffic for critical applications. Common applications that benefit from QoS are voice and video. Because voice and video applications are usually sensitive to packet loss, delay, and jitter, network devices should ensure that processing of voice and video traffic takes precedence over other less sensitive or less critical applications, especially during network congestion where packet loss, delay, and jitter may occur.

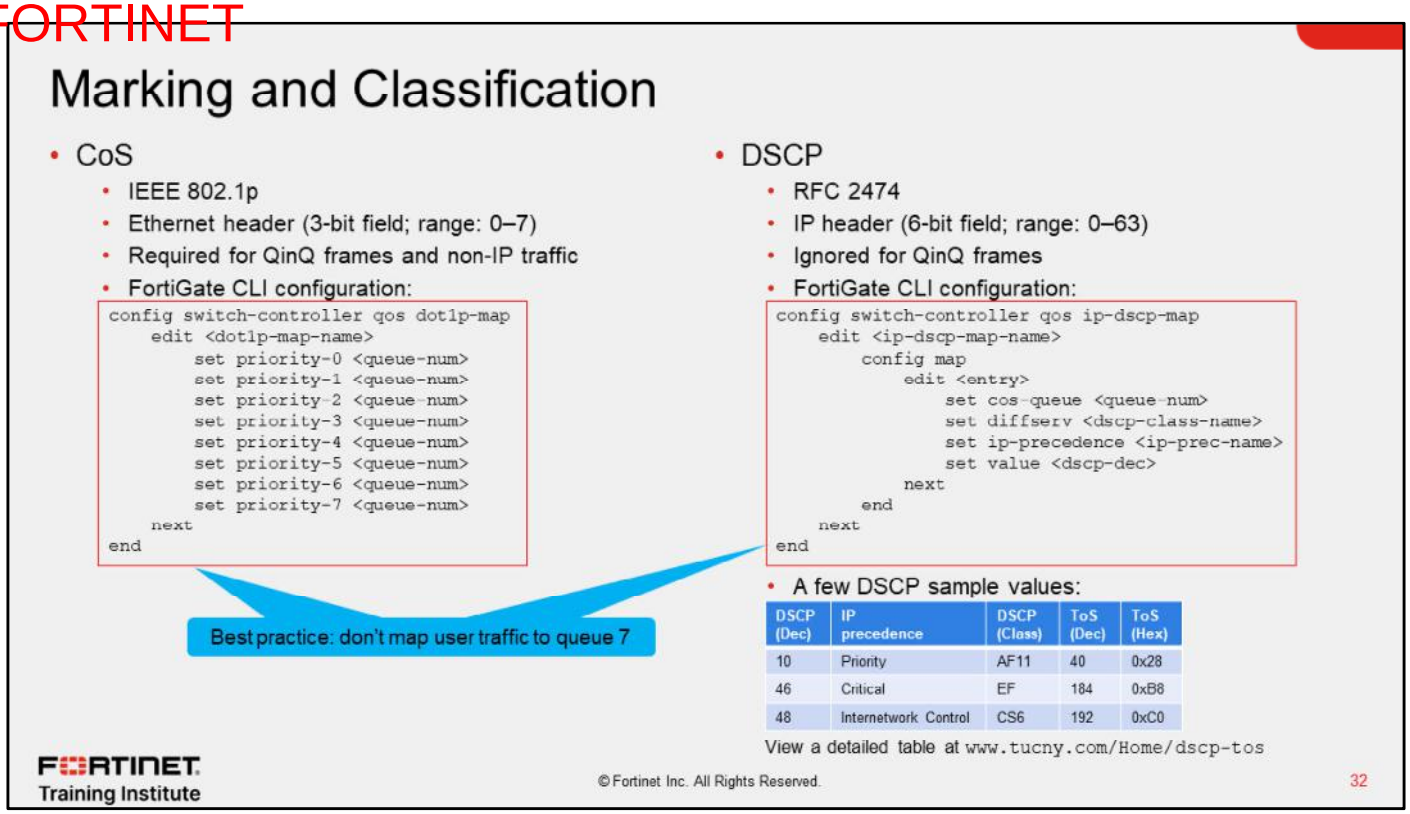
FortiSwitch supports QoS by offering the following mechanisms:

- Marking: FortiSwitch trusts the existing class of service (CoS) or Differentiated Services Code Point (DSCP) markings in a packet, or can apply new ones (also known as remarking), using access control lists (ACLs). You will learn more about ACLs in another lesson.
- Classification: FortiSwitch maps packets with a given CoS or DSCP marking to an egress queue. There are eight egress queues on each port: queues 0 to 7.
- Queuing: FortiSwitch processes packets based on the scheduling mode configured, and egress queue priority. During severe congestion on the egress port, FortiSwitch may drop packets from an egress queue based on the drop policy configured on the queue.
- Rate limiting: FortiSwitch drops traffic exceeding the configured maximum rate, but not the traffic below the minimum rate.

Note that FortiSwitch marks and classifies packets entering a port (ingress traffic), and applies queuing and rate limiting on packets leaving a port (egress traffic). The topology on this slide shows a basic QoS example. port3 on FortiSwitch is congested on the egress direction. FortiSwitch places voice packets from FortiFone on queue 6, which has the highest priority. When processing egress traffic on port3, FortiSwitch expedites voice packets sent by FortiFone to the detriment of non-voice packets sent by the PC, which are classified as low priority, and therefore dropped.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure CoS and DSCP mappings on a port for ingress traffic. Ingress packets that don't match the trusted CoS and DSCP mappings set on a port are placed in queue 0. Similarly, if no trusted CoS or DSCP mappings are set on a port, all ingress traffic on that port is placed in queue 0. In addition, by default, control traffic, such as FortiLink and LLDP is assigned to queue 7. Because control traffic should be expedited before any other traffic, it is a best practice to map user traffic to queues other than queue 7.

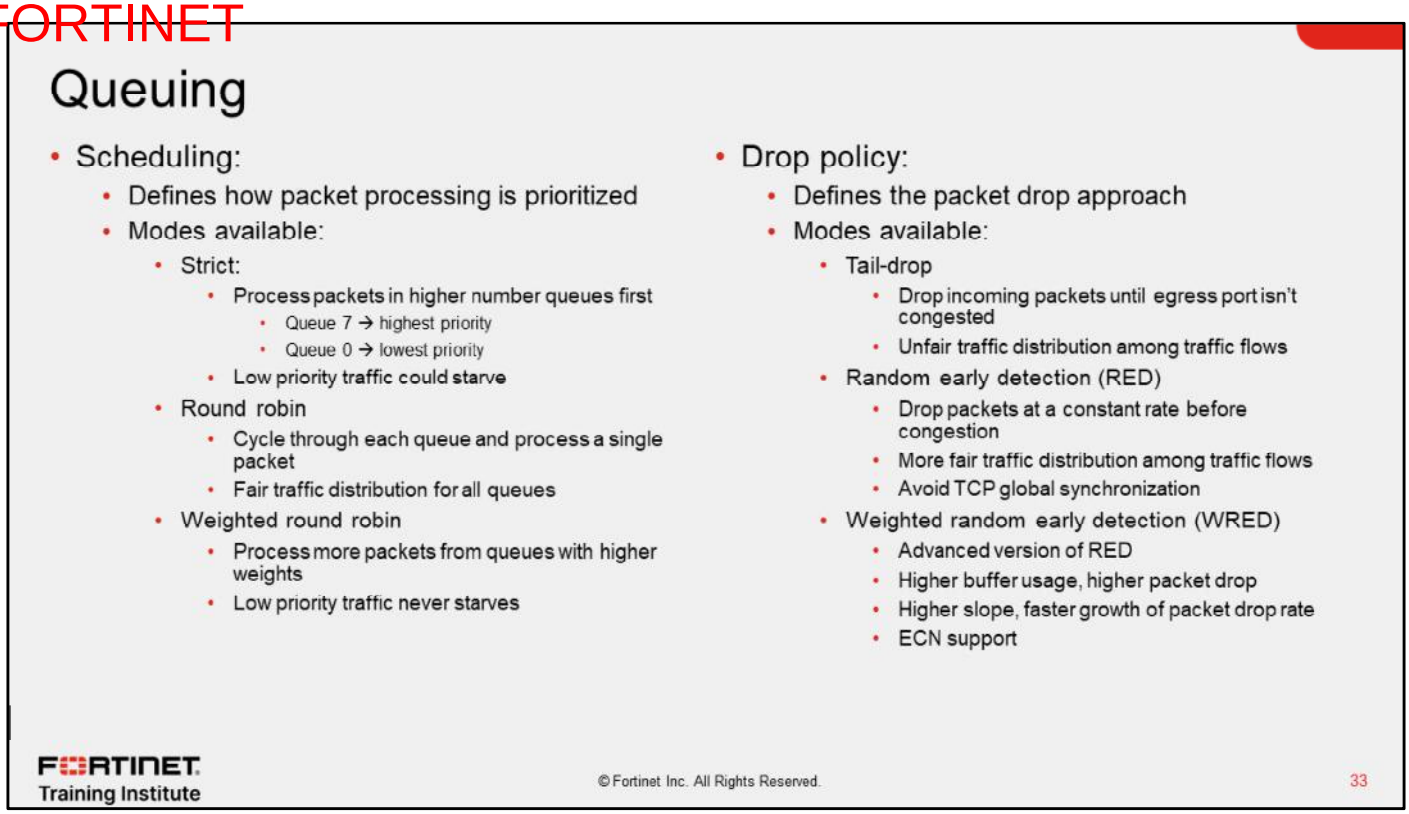
CoS is a 3-bit field in the VLAN tag of an Ethernet frame and defined in IEEE 802.1p. CoS is required for QoS classification if the frame is a QinQ or a non-IP frame. When FortiSwitch processes a QinQ frame, FortiSwitch doesn't look at its inner packet, which contains the IP header information and, therefore, the DSCP value. There are eight possible decimal values—known as priorities—in CoS: 0 to 7. When you configure the CoS mapping, you assign a priority to a queue. You can assign different CoS priorities to the same queue.

DSCP is a 6-bit field in the IP header of an IP packet and defined in RFC 2474. Unless traffic uses QinQ tagging, DSCP is usually the best QoS marking to rely on because virtually all applications use IP as the Layer 3 protocol. By contrast, not all frames are transmitted with a VLAN tag in the network, which means that CoS may not be present.

There are 64 possible decimal values in DSCP: 0 to 63. When you configure the DSCP mapping, you indicate the DSCP value using one out of three value types available: DSCP class name, IP precedence, and DSCP decimal value. You then map the DSCP value to a queue. The table on this slide shows three different DSCP decimal values and the equivalent values for a few other value types. Type of Service (ToS; RFC 1349) is the predecessor to DSCP. ToS and DSCP share some of the bits in the IP header, but their interpretation is different. Because some applications and network devices still use ToS for QoS purposes, you may need to find out the equivalent DSCP value for a given ToS value. You can view a very detailed table showing equivalent ToS and DSCP values at `www.tucny.com/Home/dscp-tos`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After FortiSwitch trusts markings on ingress packets or remarks them, and after it classifies ingress packets into queues, FortiSwitch then prioritizes packet processing based on the configured queuing policies.

Queuing policies support the following scheduling modes:

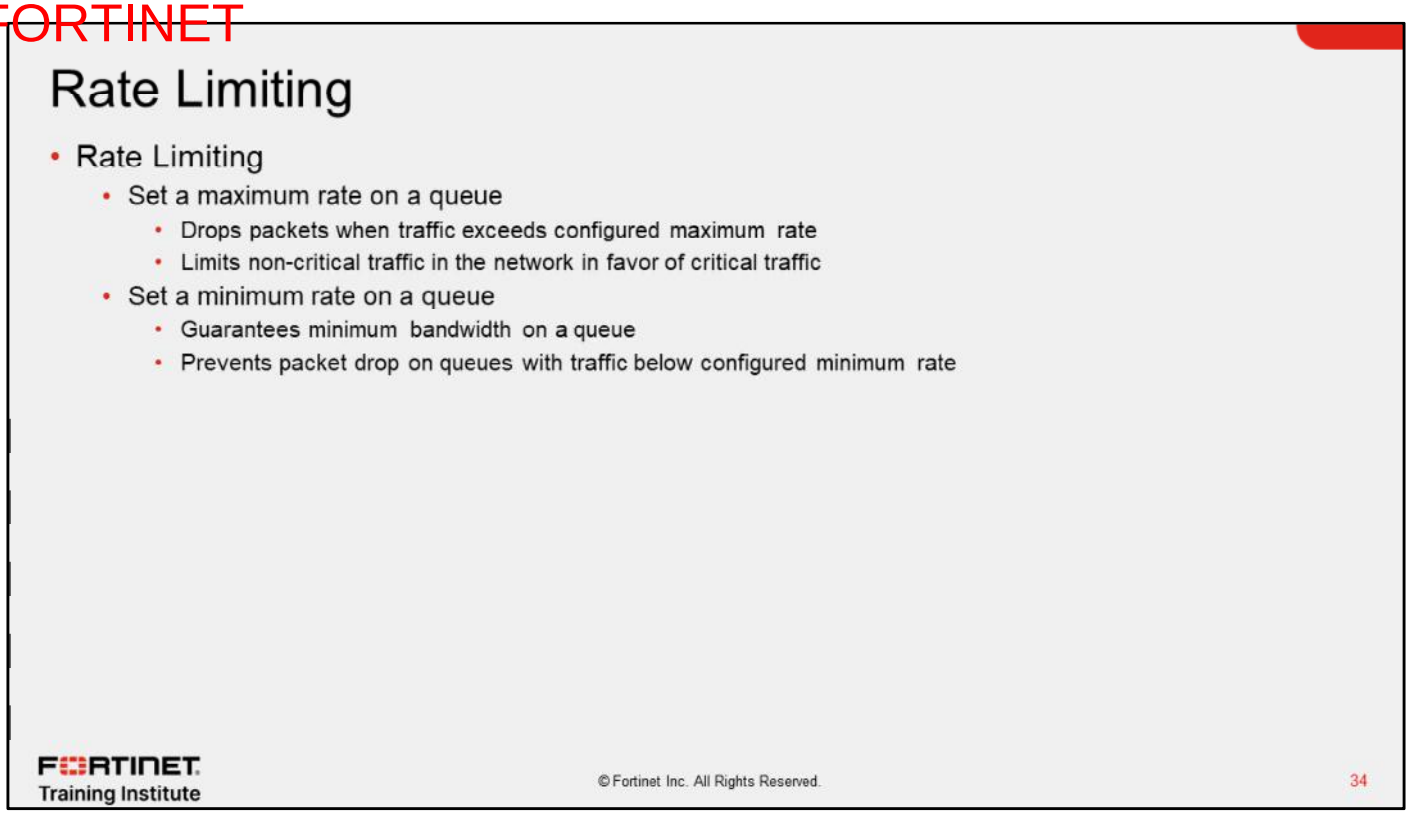
- Strict: FortiSwitch processes packets in higher number queues first before packets in lower number queues. Queue 7 has the highest priority and queue 0 the lowest. Because FortiSwitch doesn't process packets in lower queues until it finishes processing packets in higher number queues first, then this behavior may result in packets in low number queues to starve, and therefore to get dropped.
- Round robin (RR): FortiSwitch processes one packet from each queue before moving to the next one. The goal is to evenly distribute traffic from different queues.
- Weighted round robin (WRR): FortiSwitch processes more packets from queues with higher weights. Unlike strict mode, traffic assigned to lower weight queues never starve.

Before or during congestion, the switch may drop packets based on the drop policy set on the queue:

- Tail-drop: Incoming packets are dropped until there is no congestion on the egress port. With this policy, bursty traffic is less likely to be dropped, which results in unfair traffic distribution for non-bursty traffic.
- Random early detection (RED): Packets are dropped at a constant rate before congestion. The idea is to evenly drop packets from different flows and avoid TCP global synchronization, which occurs when multiple connections slow down and ramp up at the same time during congestion.
- Weighted random early detection (WRED): This is an advanced version of RED. The higher the buffer usage, the higher the packet drop. The slope setting controls the packet drop rate. The higher the slope, the faster the packet drop rate grows. You can also enable Explicit Congestion Notification (ECN) so FortiSwitch marks ECN-capable packets to signal network congestion without dropping the packets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

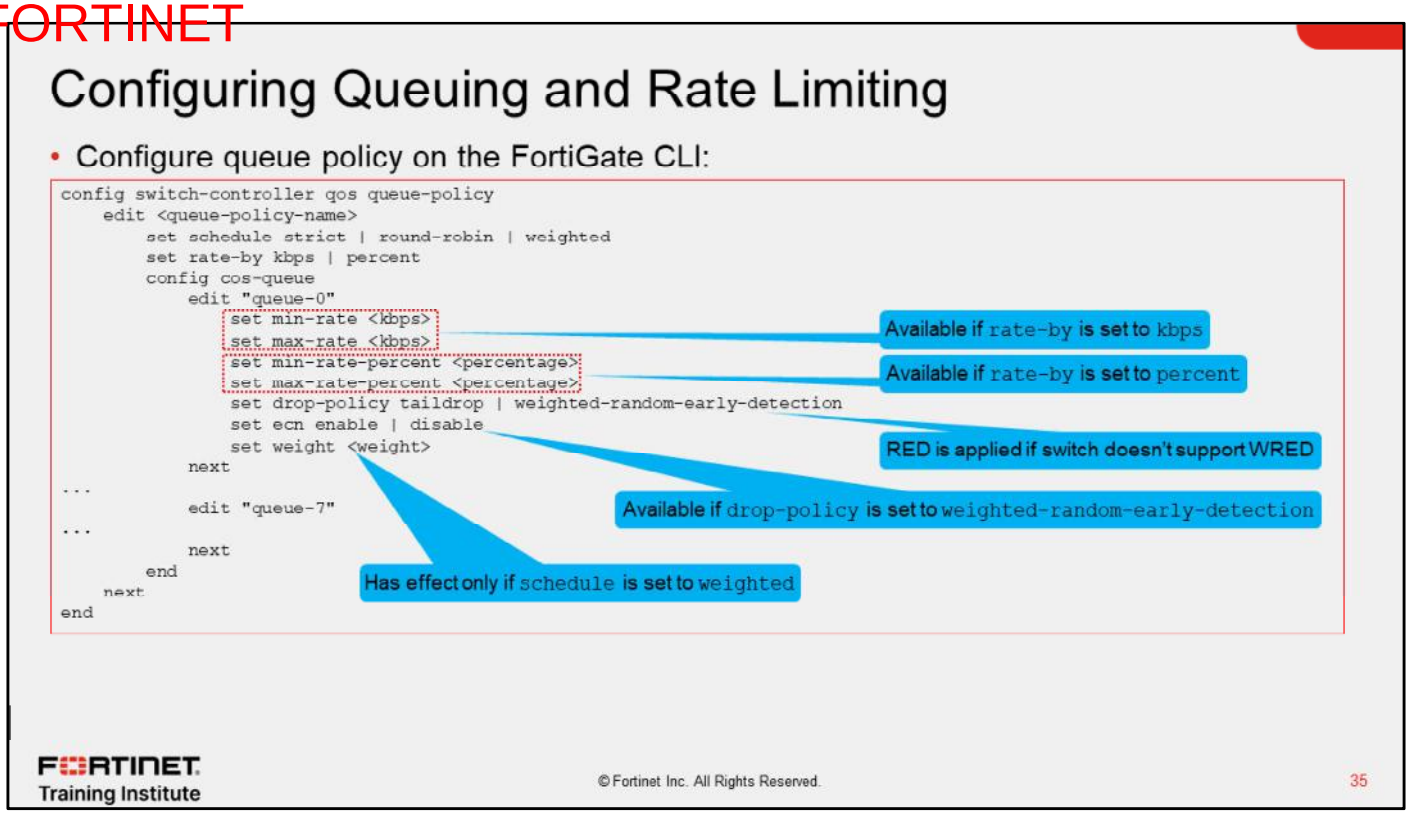


Rate limiting enables you to drop packets on a queue when the traffic exceeds the configured maximum rate on the queue. Usually, you may want to enforce a maximum rate on a low priority queue to allocate more bandwidth to traffic from high priority queues.

You can also set a minimum rate for traffic on a queue. Unlike the maximum rate that limits the traffic on a queue, the minimum rate is used to guarantee the minimum bandwidth on a queue before packets can be dropped. The goal is to skip packet drop on queues with an amount of traffic below its minimum rate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

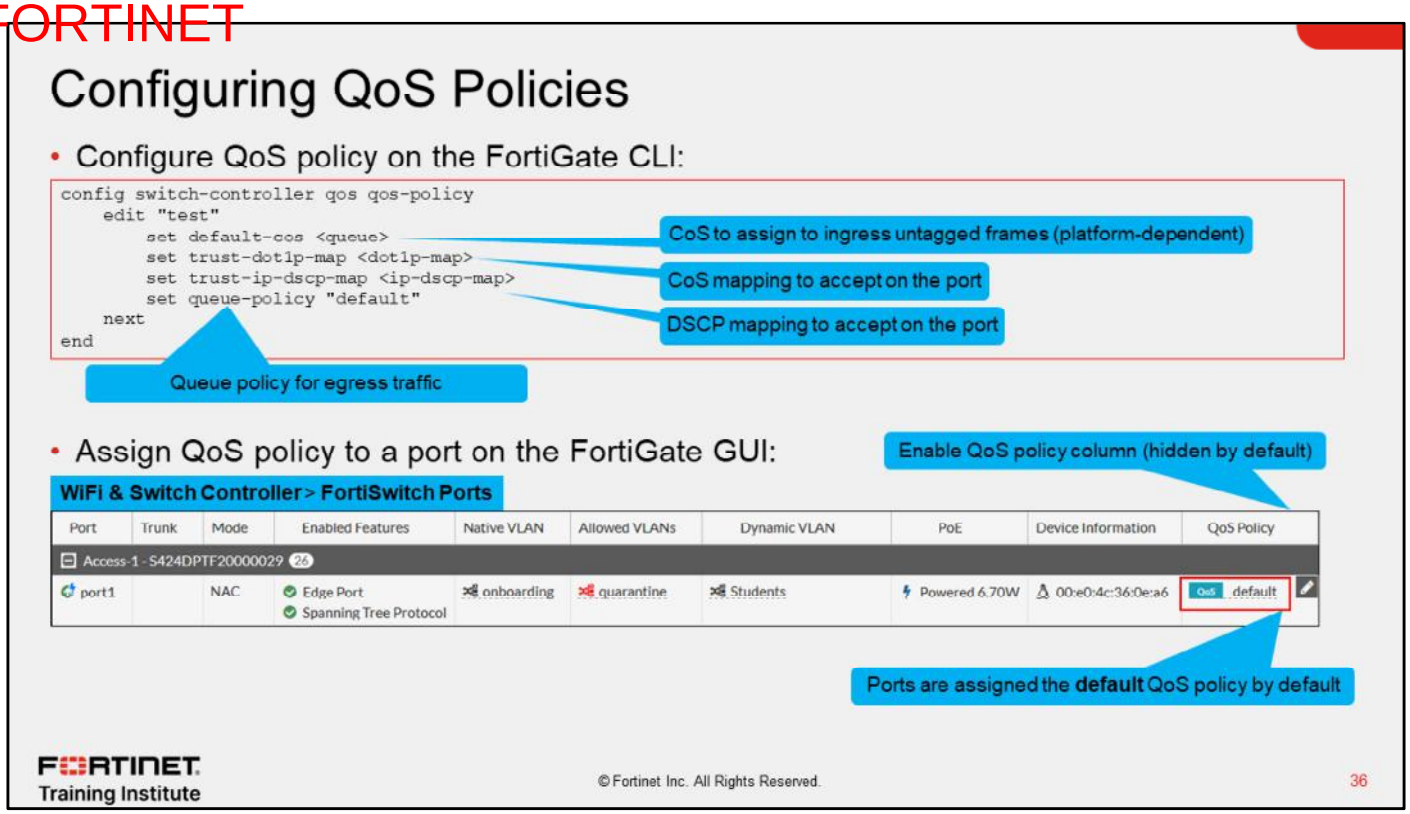


You configure queuing and rate limiting settings by creating or editing a queue policy using the FortiGate CLI.

This slide shows the different settings available in a queue policy. The type used for minimum and maximum rate settings depends on the configured `rate-by` setting. Note that FortiGate doesn't show an option to select RED as the drop policy. However, when WRED is selected as the drop policy, FortiGate applies WRED on the managed switch only if the switch supports it. Otherwise, it applies RED. Also, the `weight` setting takes effect only if `schedule` is set to `weighted`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The final step to configure QoS is to create a QoS policy, and apply it to a port. A QoS policy combines the required trusted QoS mappings and queue policy to apply on a port. Ingress packets that don't match the trusted CoS and DSCP mappings set on a port are placed in queue 0. Similarly, if no trusted CoS or DSCP mappings are set on a port, all ingress traffic on that port is placed in queue 0.

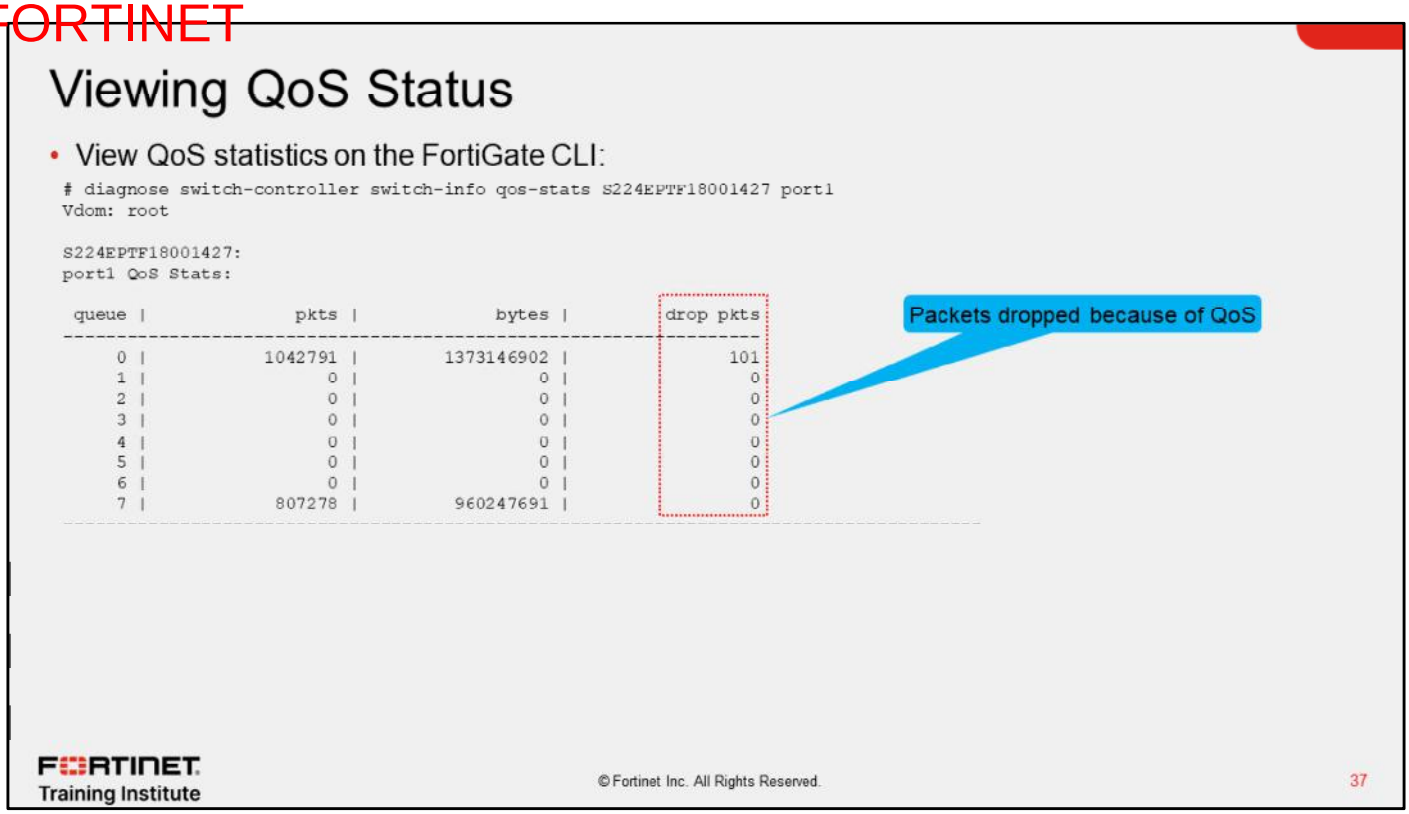
You can also define the default CoS to assign ingress untagged frames to. The default CoS is assigned internally by FortiSwitch and used when prioritizing egress traffic. Note that the `default-cos` setting is available on some FortiSwitch models only.

The selected queue policy defines how traffic is prioritized on egress, and optionally, rate limited.

After you configure the QoS policy, you can assign it on a port using the FortiGate GUI. Make sure to enable the **QoS Policy** column first, so you can select the QoS policy to assign on a port. Note that all ports are assigned the **default** QoS policy by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

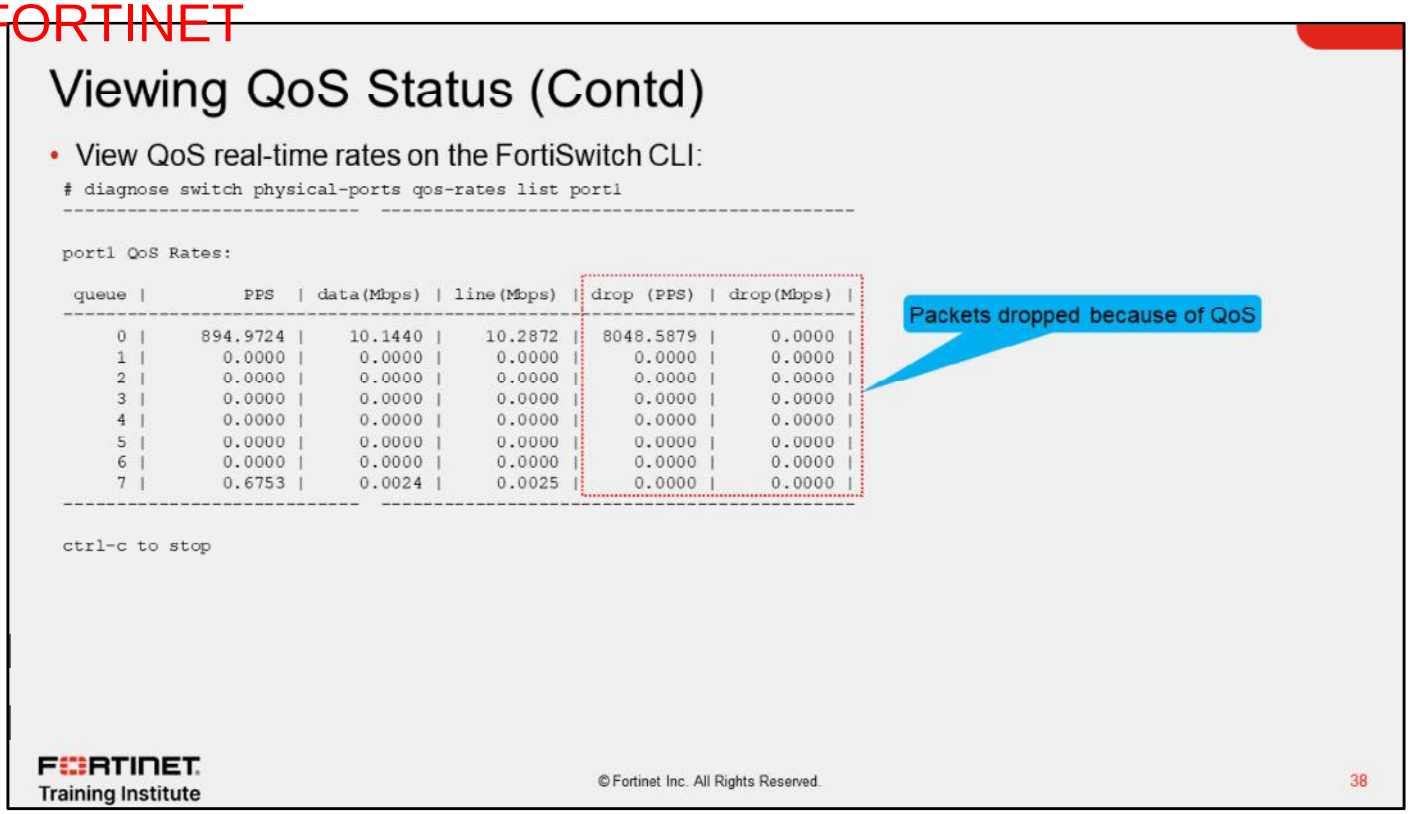
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to display QoS stats for a port on a managed switch using the FortiGate CLI. The output includes the number of packets dropped by QoS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



On FortiSwitch, you can run the CLI command shown on this slide to get the real-time QoS rates on a port. The output includes rates in both packets per second (PPS) and Mbps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about QoS in FortiSwitch is true?
   - ✓ A. FortiSwitch can remark CoS and DSCP values using ACLs.
   - B. Queuing and rate limiting are applied on ingress traffic.

2. Which drop policy provides the most unfair traffic distribution?
   - ✓ A. Tail drop
   - B. Random early detection (RED)

3. Which type of marking is ignored by FortiSwitch when processing QinQ traffic?
   - A. CoS
   - ✓ B. DSCP

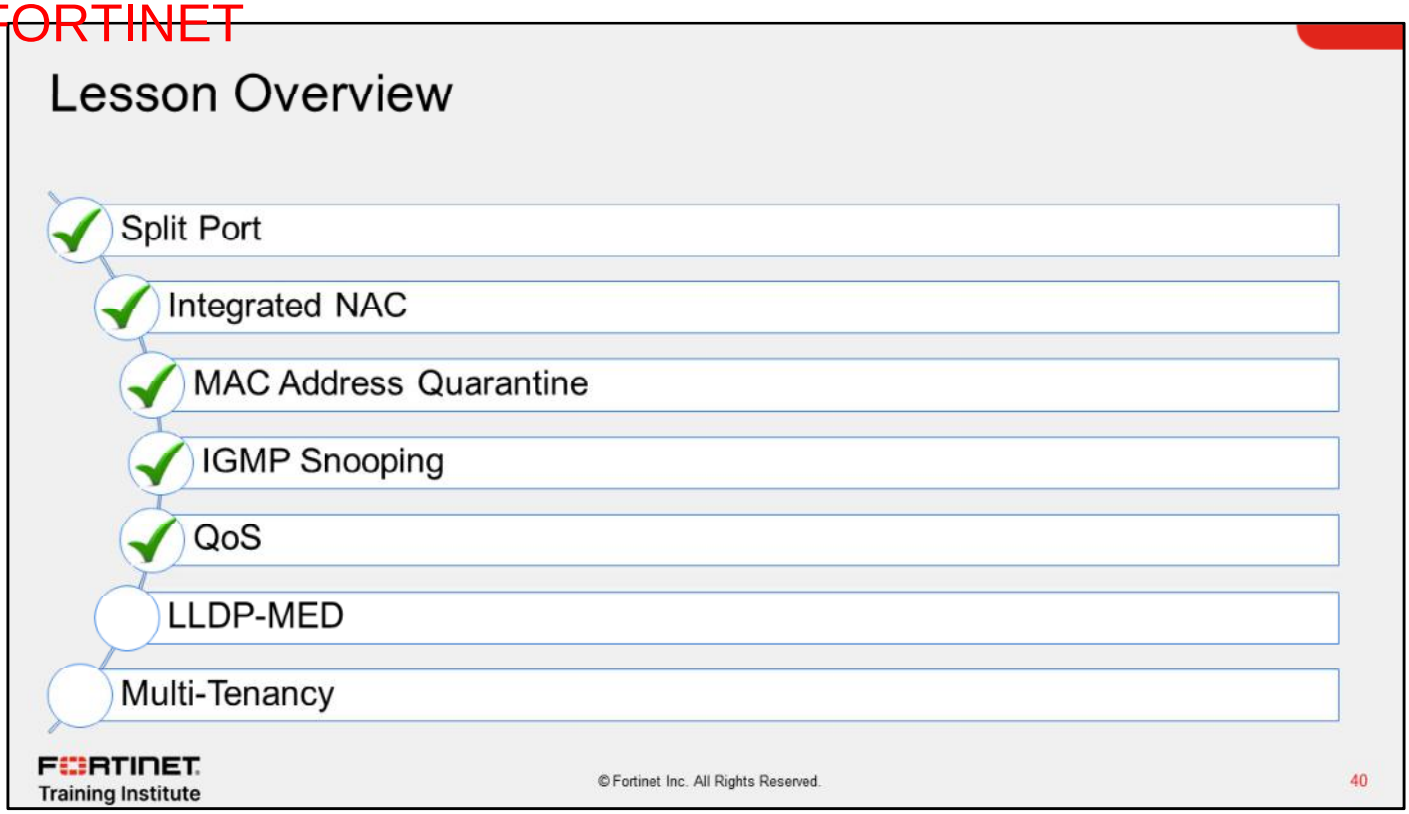
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

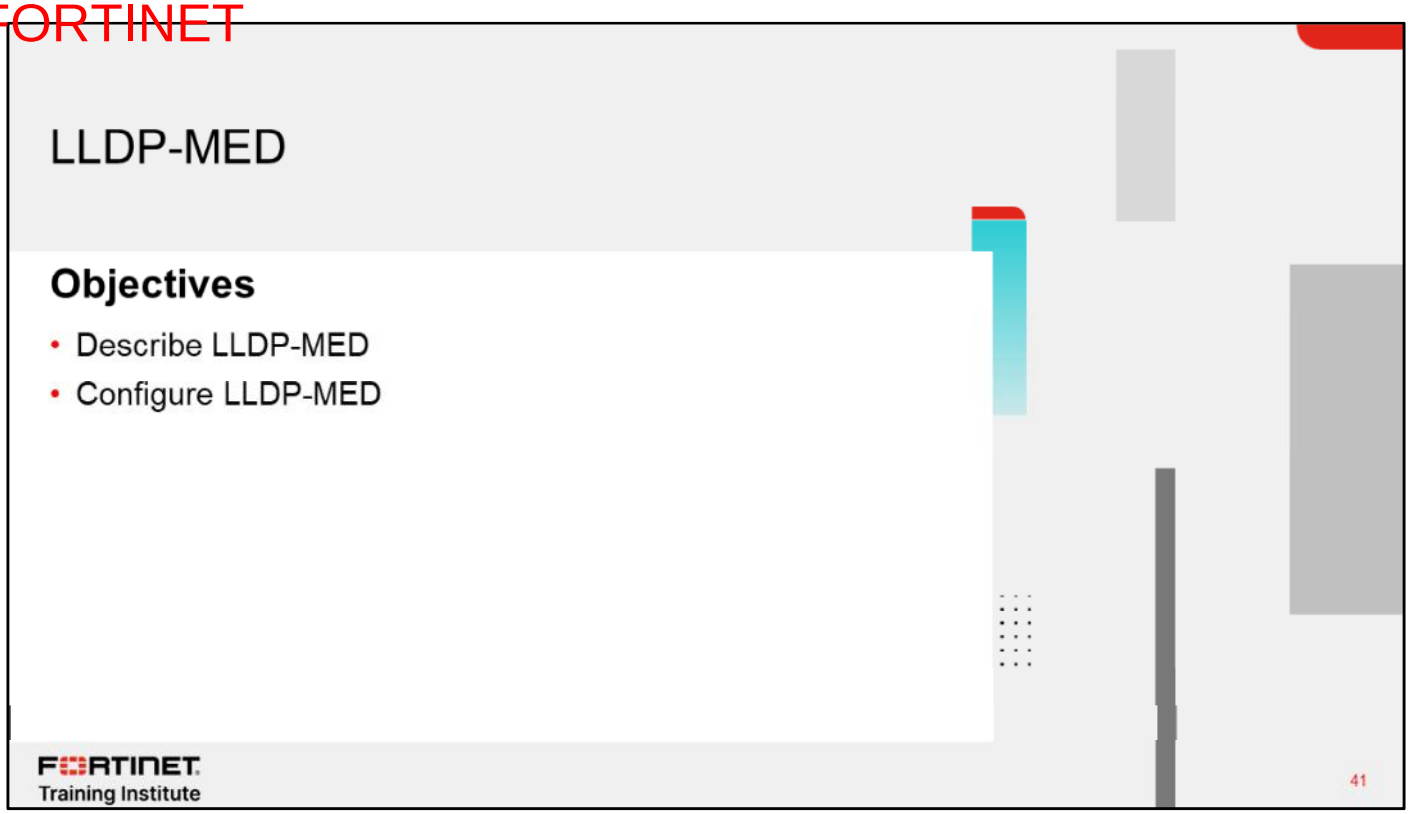


Good job! You now understand QoS.

Now, you will learn about LLDP-MED.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

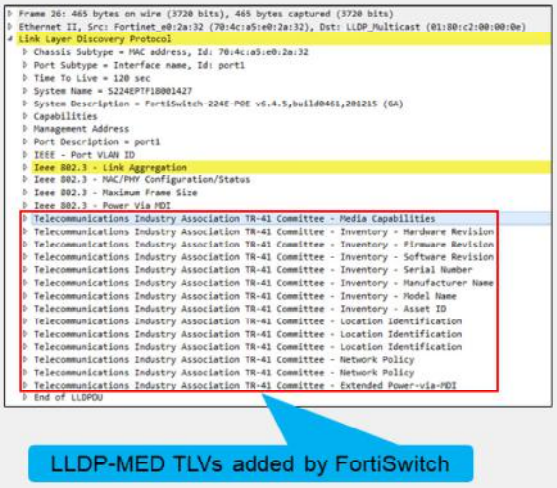
By demonstrating competence in LLDP-MED, you should be able to understand how to use LLDP-MED to simplify deployment for capable endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

LLDP-MED

- Enables endpoints to automatically learn and apply settings using LLDP-MED TLVs
  - Endpoints are usually IP phones and video-capable devices
  - Simplifies network deployment
- LLDP-MED TLVs supported by FortiSwitch:
  - Network policy
    - Endpoint learns and applies network settings for a given application
  - Location
    - Endpoint learns location details such as coordinates, civic address, and ELIN
  - Power management
    - Endpoint advertises power information and negotiates power allocation
  - Inventory management
    - Endpoint advertises detailed device information



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

LLDP-Media Endpoint Discovery (LLDP-MED) is an extension to LLDP that enables endpoints that support LLDP-MED, usually IP phones and video-capable devices, to obtain information from an adjacent LLDP device, usually a switch, and use that information for autoconfiguration purposes. For example, a switch can use LLDP-MED Type-Length-Values (TLVs) to advertise the QoS markings and VLAN that connected IP phones should use for voice and signaling traffic. IP phones can then apply such settings automatically, thus making network deployment easier. In addition, a switch can also use the additional LLDP-MED TLVs sent by endpoints to collect detailed information about connected devices for inventory management purposes.

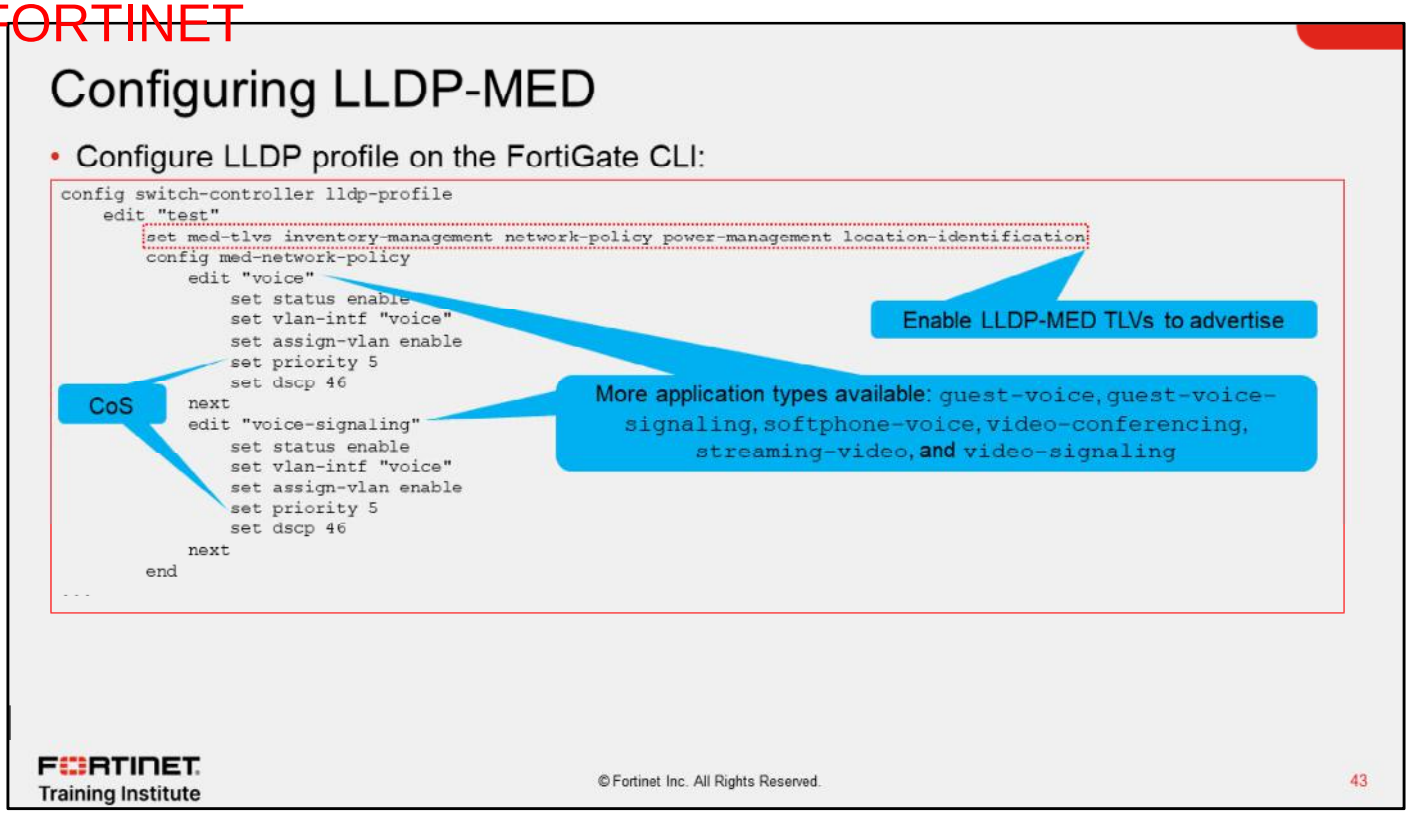
FortiSwitch supports the following LLDP-MED TLVs:

- Network policy: enables endpoints to learn network settings, such as CoS, DSCP, and VLAN, for a given application like voice and voice signaling. The goal is for endpoints to automatically adjust their settings based on the network policies advertised by FortiSwitch.
- Location: FortiSwitch can advertise location details such as the coordinates and civic address. FortiSwitch can also advertise the emergency location identifier number (ELIN) of the location. The ELIN is used to provide specific location information to the public safety answering point (PSAP) during a 911 call.
- Power management: enables PoE-capable switches and endpoints to advertise power information and negotiate power allocation.
- Inventory management: FortiSwitch collects detailed information about endpoints, enabling network administrators to track their network devices and determine their characteristics.

This slide shows an LLDP frame on Wireshark that was advertised by FortiSwitch. The image highlights the LLDP-MED TLVs that FortiSwitch adds to the standard LLDP frame when you enable all the supported LLDP-MED TLVs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



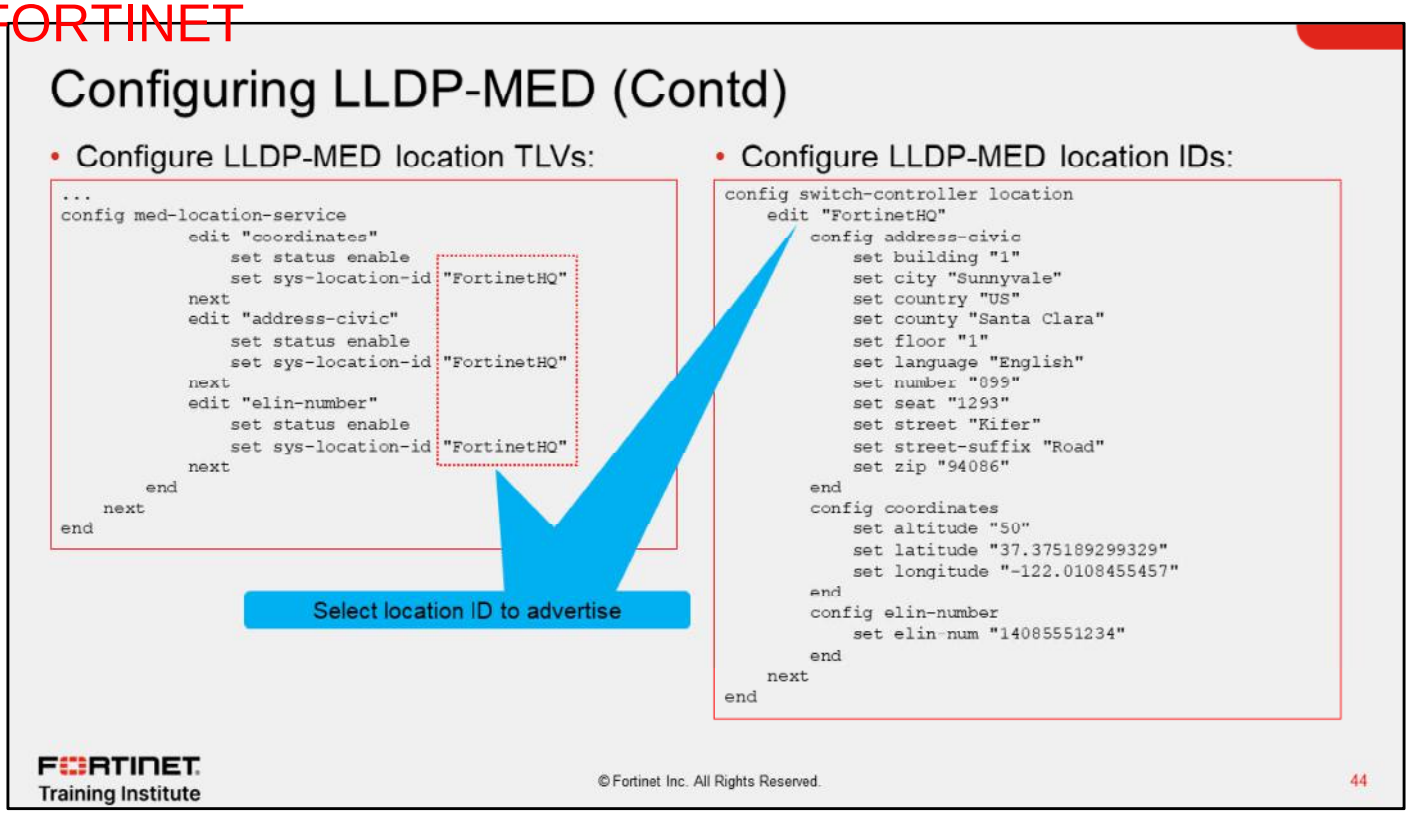
You configure LLDP-MED by enabling the corresponding TLVs on the LLDP profile using the FortiGate CLI. This slide shows the first part of a sample LLDP profile named `test`. The first step in the configuration is to select which LLDP-MED TLVs to advertise. All four supported LLDP-MED TLVs are enabled.

After that, you configure the network policy settings for each application type. The example shows `voice` and `voice-signaling` as the only application types configured, but you can also configure the following application types: `guest-voice`, `guest-voice-signaling`, `softphone-voice`, `video-conferencing`, `streaming-video`, and `video-signaling`.

Note that for each network policy, the VLAN, DSCP, and CoS (priority) are set.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The second part of the sample LLDP profile shows the LLDP-MED location TLV configuration. You first enable which location TLVs you want to advertise, and then select the location ID that contains the location information contained in the location TLVs.

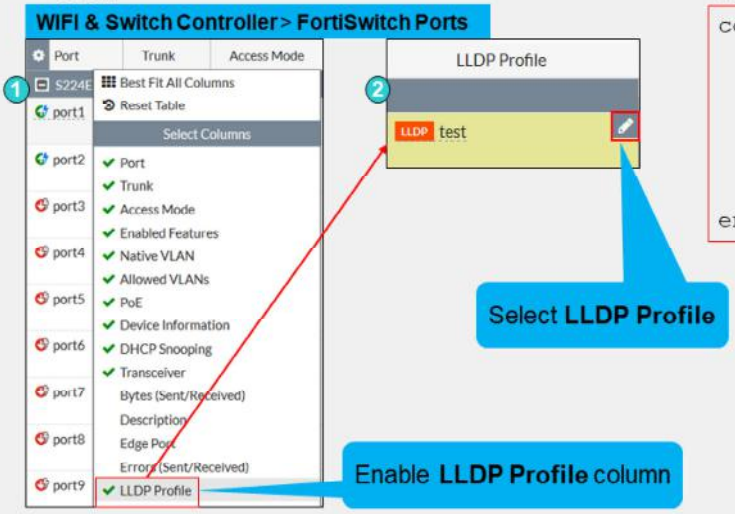
The location ID is configured on a different configuration subsection on the FortiGate CLI, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Applying LLDP Profiles

- To apply an LLDP profile on the FortiGate GUI:



- To apply an LLDP profile on the FortiGate CLI:

```
config switch-controller managed-switch
    edit <switch-id>
        config ports
            edit <port>
                set lldp-profile <profile>
            next
    next
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

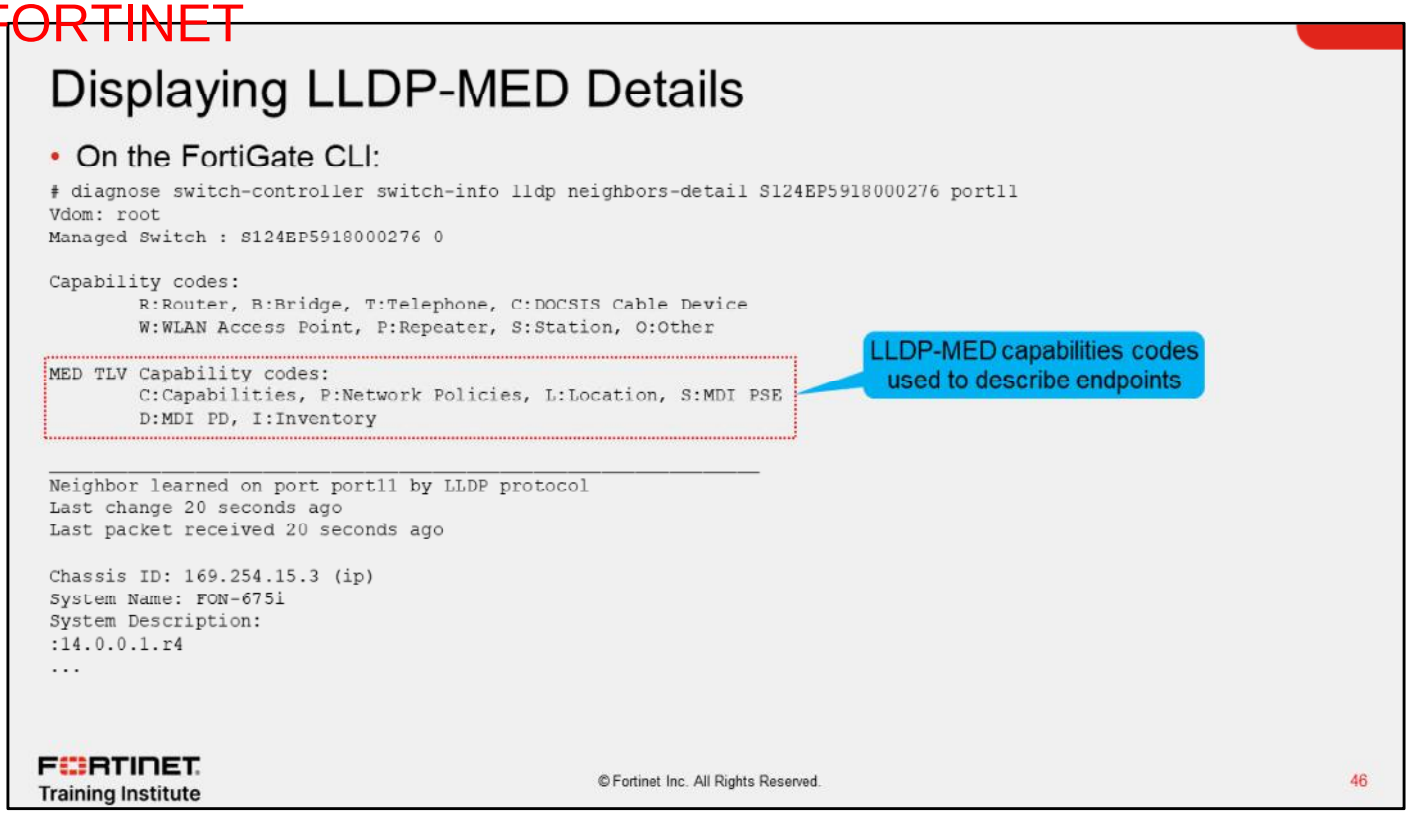
45

You can apply LLDP profiles on the **FortiSwitch Ports** page. First, you must enable the **LLDP Profile** column. Then, hover over the setting, click the pencil icon, and then select the LLDP profile from a list.

Alternatively, you can apply an LLDP profile on the FortiGate CLI, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

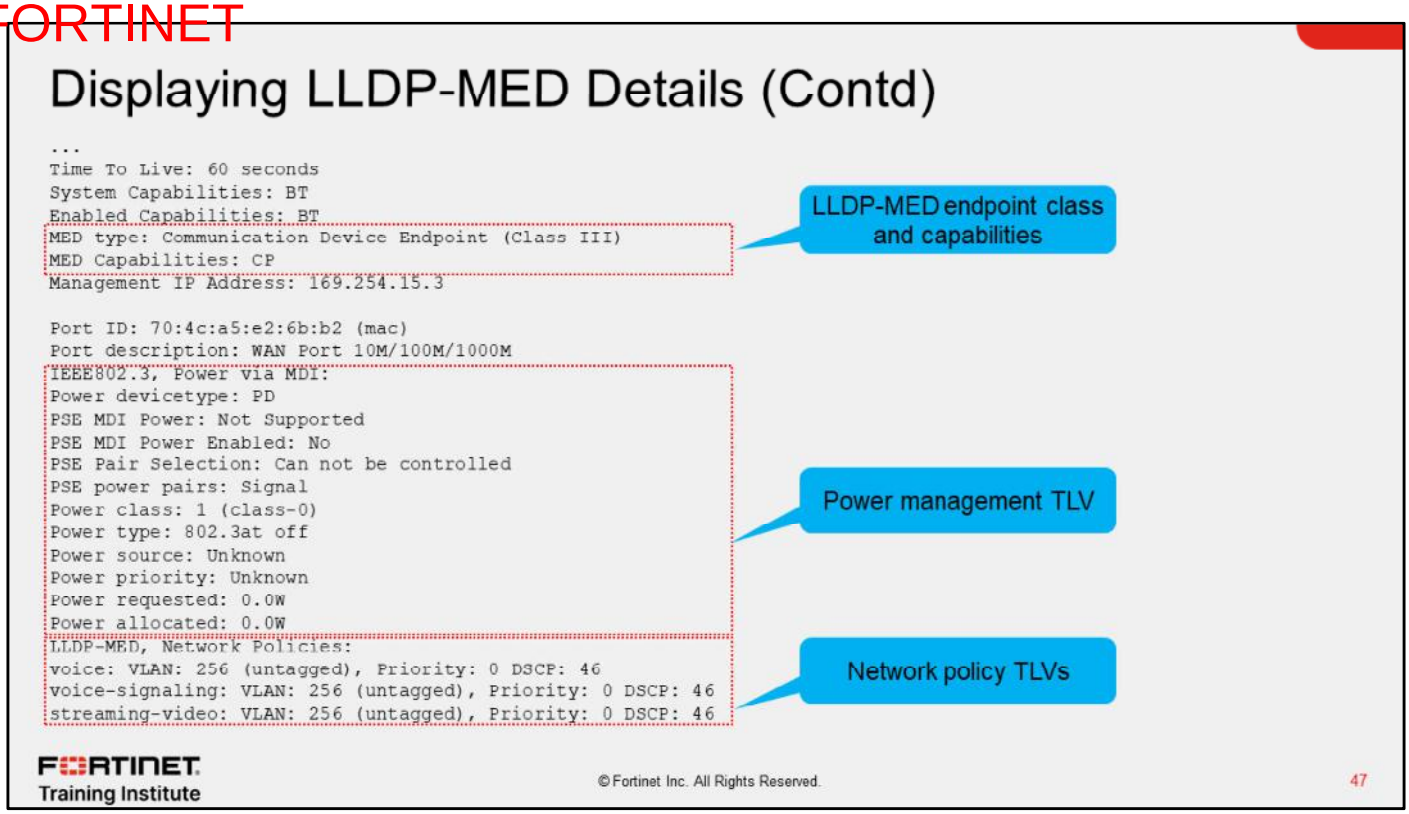
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The LLDP-MED neighbor information can be found in the same output of the LLDP neighbor details command. This slide shows the first part of the output taken for a FortiFone 675i endpoint, which is an IP phone from Fortinet that supports LLDP-MED. At the beginning of the output, there is a legend describing the different LLDP-MED TLV capability codes for your reference.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the second part of the sample LLDP neighbor details output for a FortiFone 675i. This part of the output shows specific LLDP-MED TLVs such as power management and network policies. The output also indicates the class of the LLDP-MED endpoint connected and its capabilities. There are three endpoint classes defined in LLDP-MED. Class III is advertised by devices classified as communication endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about LLDP-MED is true?

✓A. You can assign network settings on endpoints that support LLDP-MED by using network policy TLVs.

B. LLDP-MED TLVs are transmitted in separate frames from the standard LLDP frames.

2. What is the location LLDP-MED TLV used for?

✓A. It enables endpoints to learn from FortiSwitch the coordinates, civic address, and ELIN of the location.

B. It enables FortiSwitch to collect detailed device information for inventory management purposes.

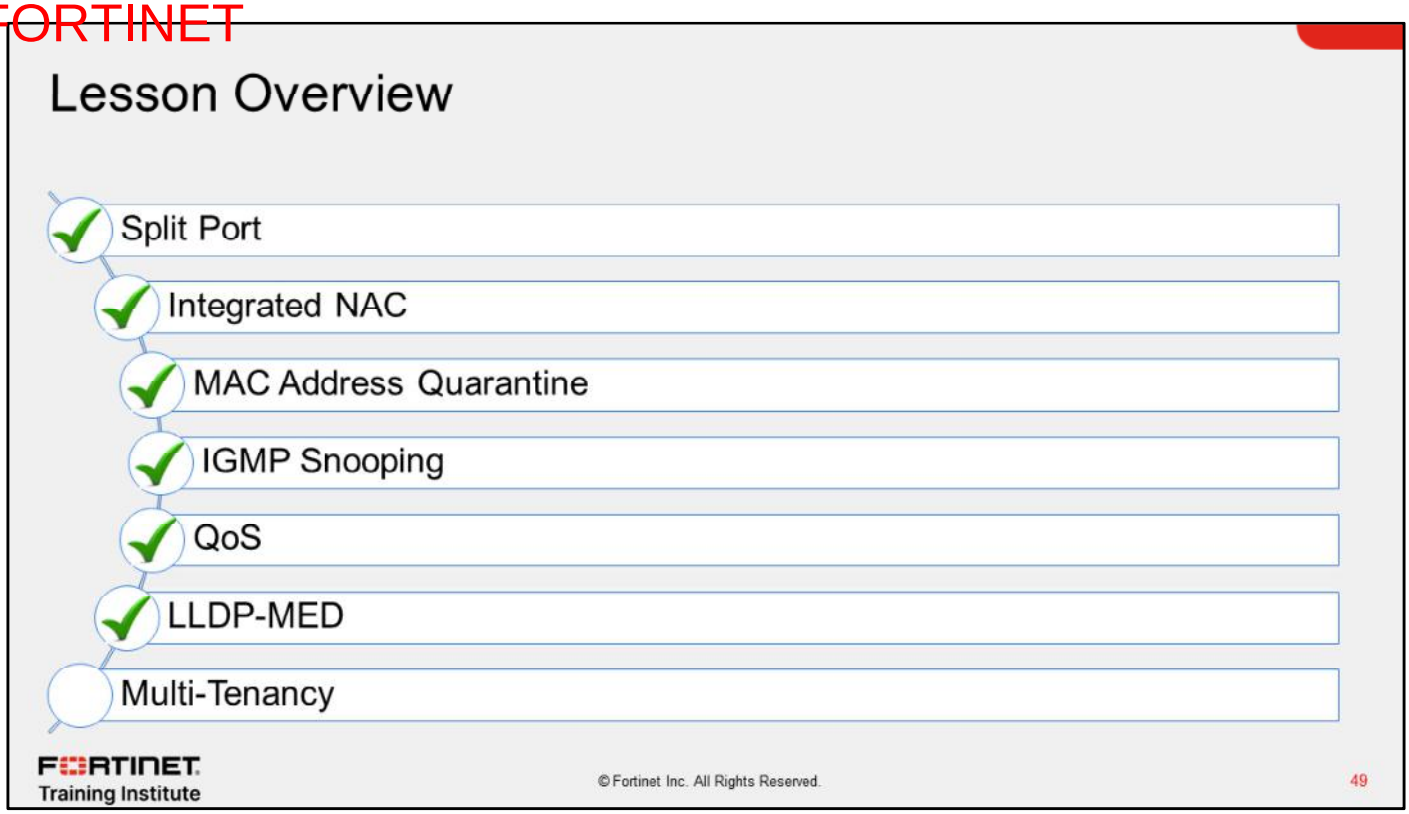
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

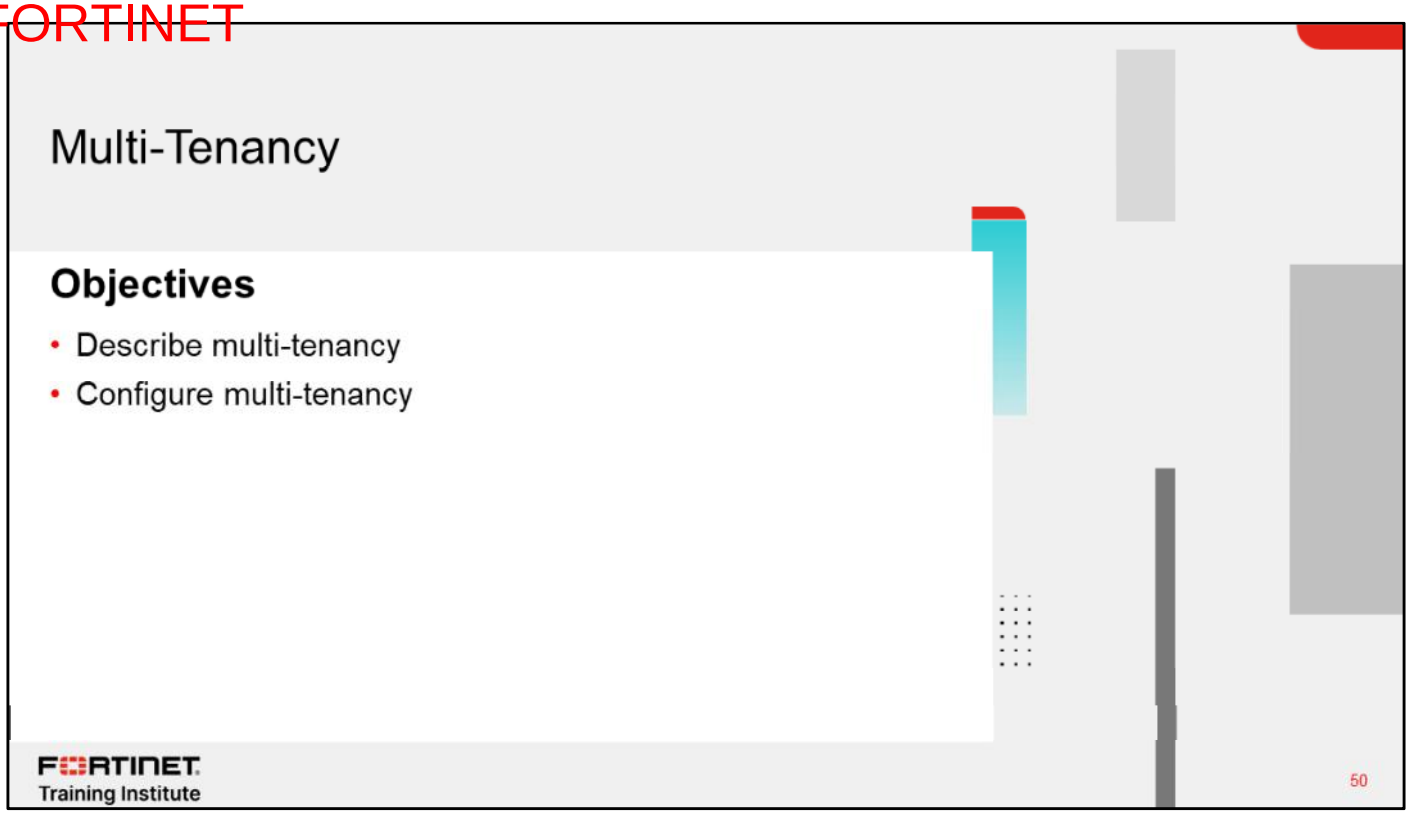


Good job! You now understand LLDP-MED.

Now, you will learn about multi-tenancy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

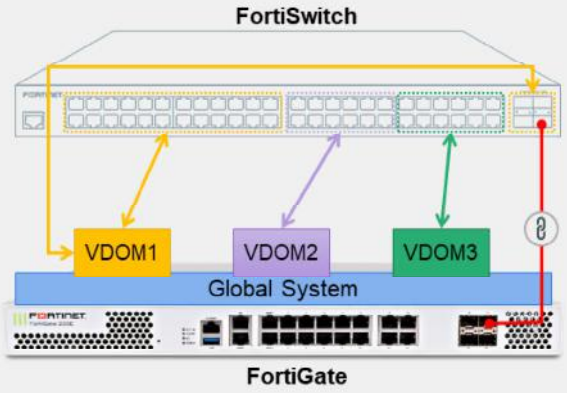
By demonstrating competence in multi-tenancy, you should be able to understand how to assign FortiSwitch ports to VDOMs without having to deploy additional managed FortiSwitch stacks or make extra physical connections.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Multi-Tenancy

- Assign FortiSwitch ports to different VDOMs
  - Segment management of FortiSwitch ports
    - Useful for MSSPs and similar network deployments
  - Cost-effective, no need to:
    - Create additional FortiLink interfaces
    - Make extra physical connections
- Limitations:
  - No support for:
    - LLDP
    - STP
    - BPDU guard
    - Root guard
    - DHCP snooping
    - IGMP snooping
    - MCLAG
    - MAC address quarantine



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

51

FortiGate allows you to create VDOMs to divide your FortiGate into multiple logical devices. This logical segmentation on FortiGate is useful for MSSP and businesses with network deployments alike because it enables them to segment the network operation and its management.

So, what if you also wanted to segment FortiSwitch devices across multiple VDOMs? One option is to have a FortiLink interface per VDOM. This approach requires you to deploy multiple FortiSwitch stacks, each of them with a separate physical connection to the VDOM FortiLink interface. A more cost-effective option is to use the FortiGate multi-tenancy feature for managed FortiSwitch stacks.

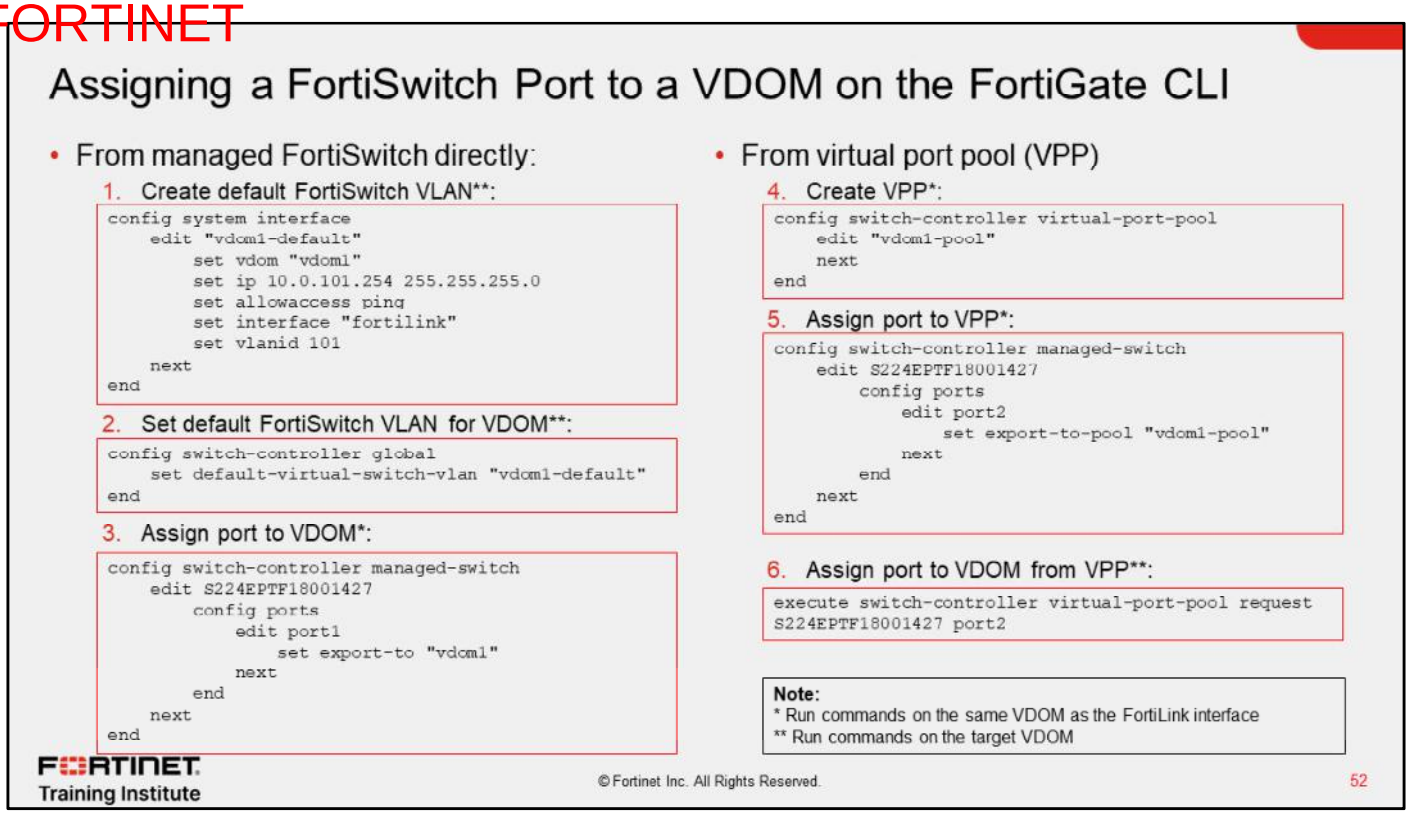
Multi-tenancy *for managed FortiSwitch* enables you to assign ports of your existing FortiSwitch stack to a different VDOM from the VDOM the FortiLink interface is configured on. You don't need to create additional FortiLink interfaces or make extra physical connections. You just have to assign a port to a VDOM, and then the port becomes available on the target VDOM for use.

Note that you can't use any of the features listed on this slide on a port that have been assigned to a different VDOM using multi-tenancy.

The example on this slide shows FortiGate with three VDOMs configured. Although the FortiLink interface is created on VDOM1, you can still assign ports of the managed FortiSwitch to VDOM2 and VDOM3.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



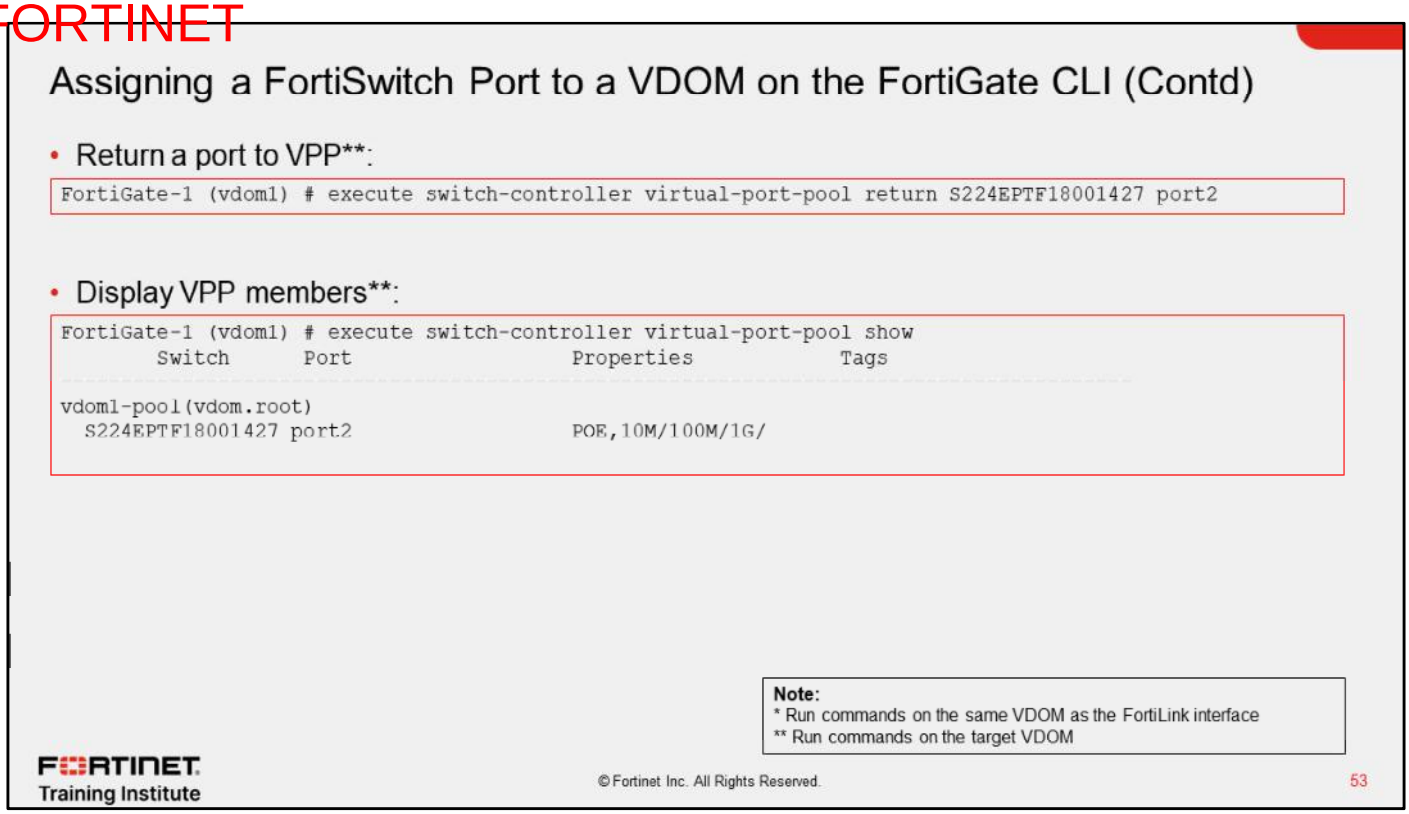
This slide shows an example of how to assign a port to a VDOM directly or by using a virtual port pool (VPP) on the FortiGate CLI. The target VDOM is `vdom1`. Port1 is assigned directly to `vdom1`, and port2 indirectly from a VPP.

When using a VPP, you first indicate a group of ports that can be assigned to other VDOMs. VDOM-specific administrators can then pick one or more of those ports and use them for their respective VDOMs.

Note that you must execute some commands on the same VDOM where the FortiLink interface is configured, and others on the target VDOM that you want to assign the ports on.

Vouchers & Dumps are Available | WhatsApp +201224560923

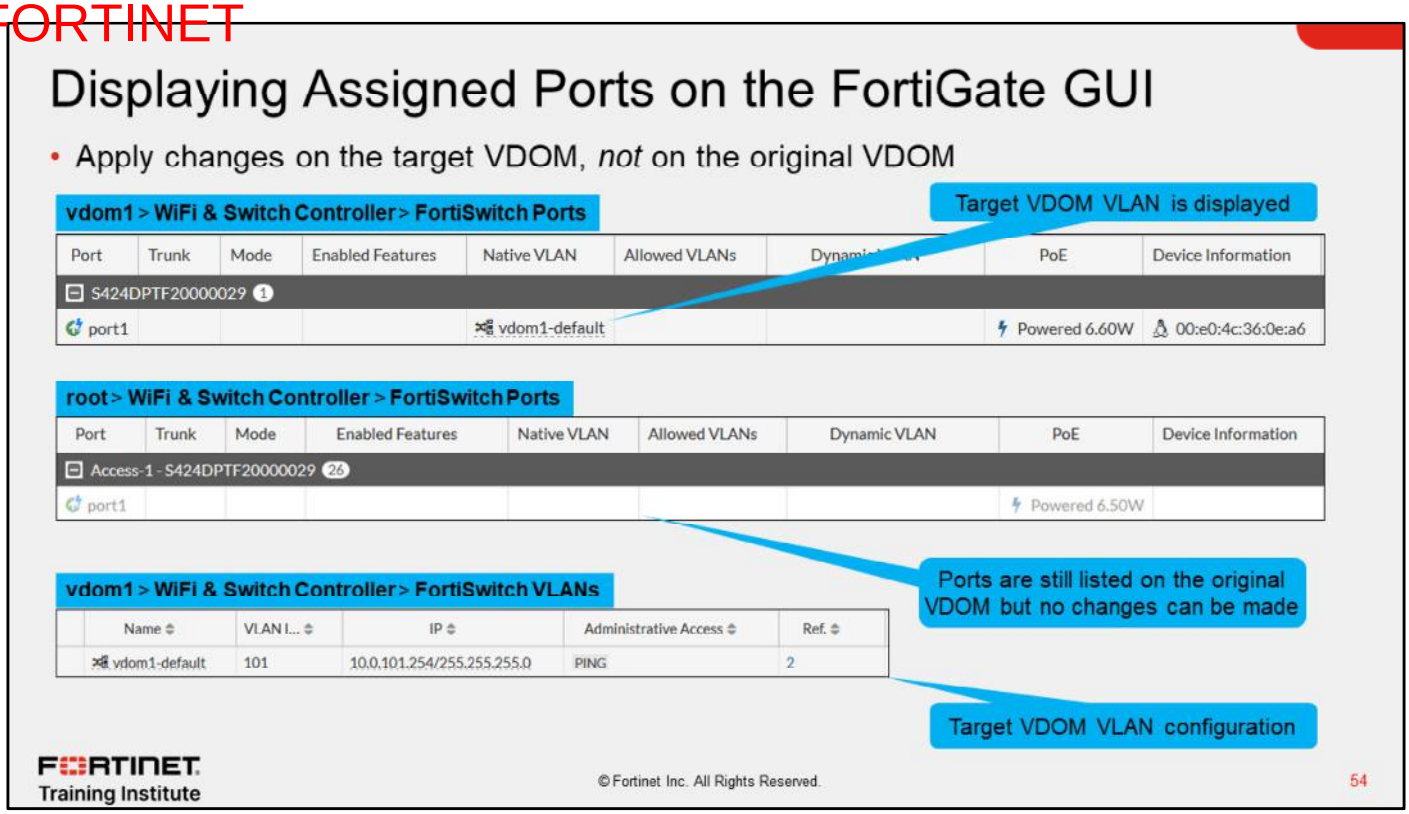
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also assign a port back to its pool by running the command shown on this slide. You can also display the current members of a VPP, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you assign ports to the target VDOM (vdom1), you are still able to see the ports on the original VDOM (root). However, no changes can be made on the root VDOM for the ports that have been assigned to another VDOM. You must configure the ports directly on the vdom1 VDOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about multi-tenancy for managed FortiSwitch devices is true?
   - A. STP is supported on the port that is assigned to the target VDOM.
   - ✓ B. It doesn't require additional FortiLink interfaces or physical connections.

2. On which VDOM must you apply the configuration for assigned ports?
   - ✓ A. The target VDOM of the port.
   - B. The original VDOM of the port.

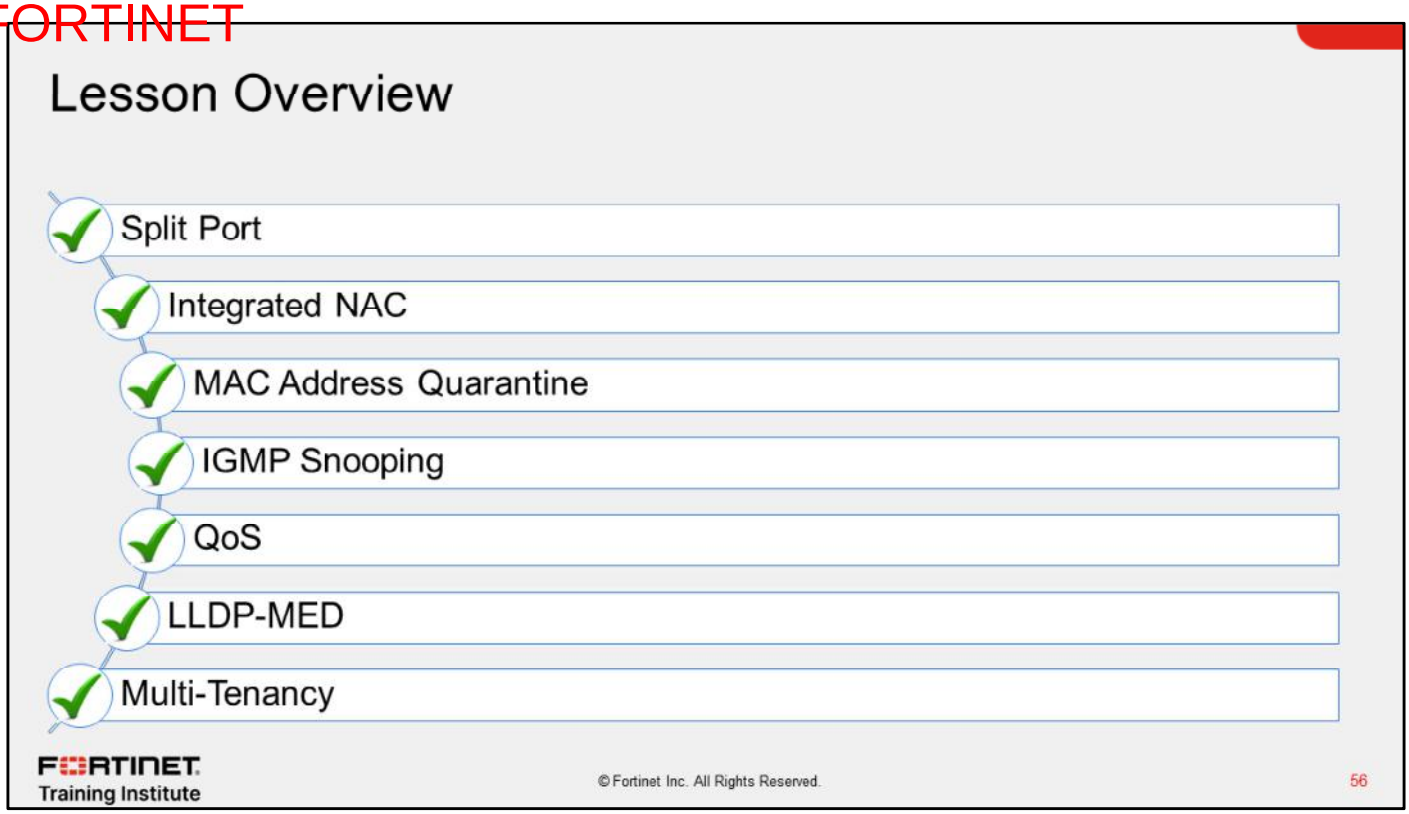
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

55

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

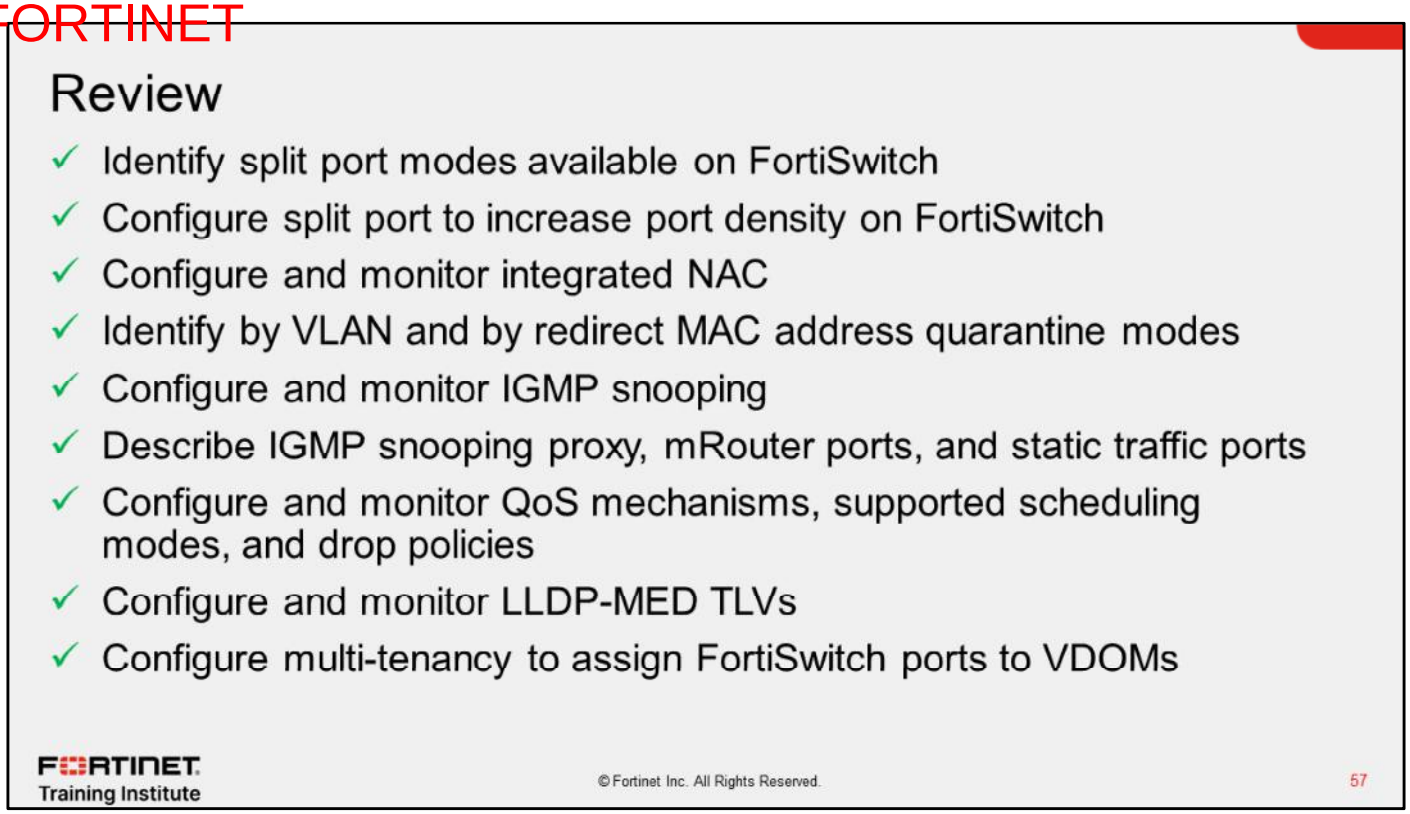


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

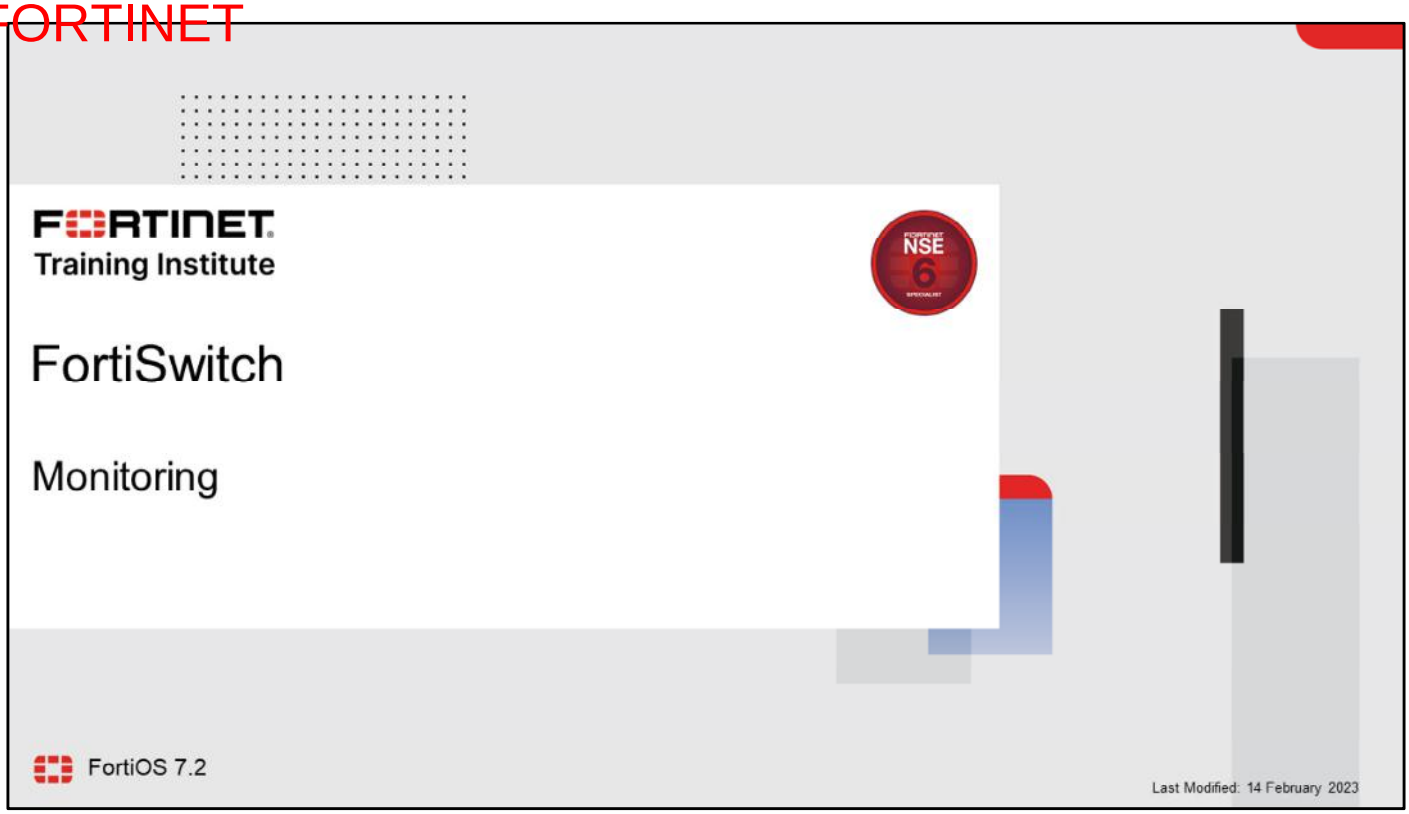


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the different advanced features that you can enable on your managed FortiSwitch stack to increase port density, automate and simplify endpoint deployment, isolate compromised endpoints at Layer 2, prioritize critical traffic, and assign FortiSwitch ports to VDOMs.

Vouchers & Dumps are Available | WhatsApp +201224560923

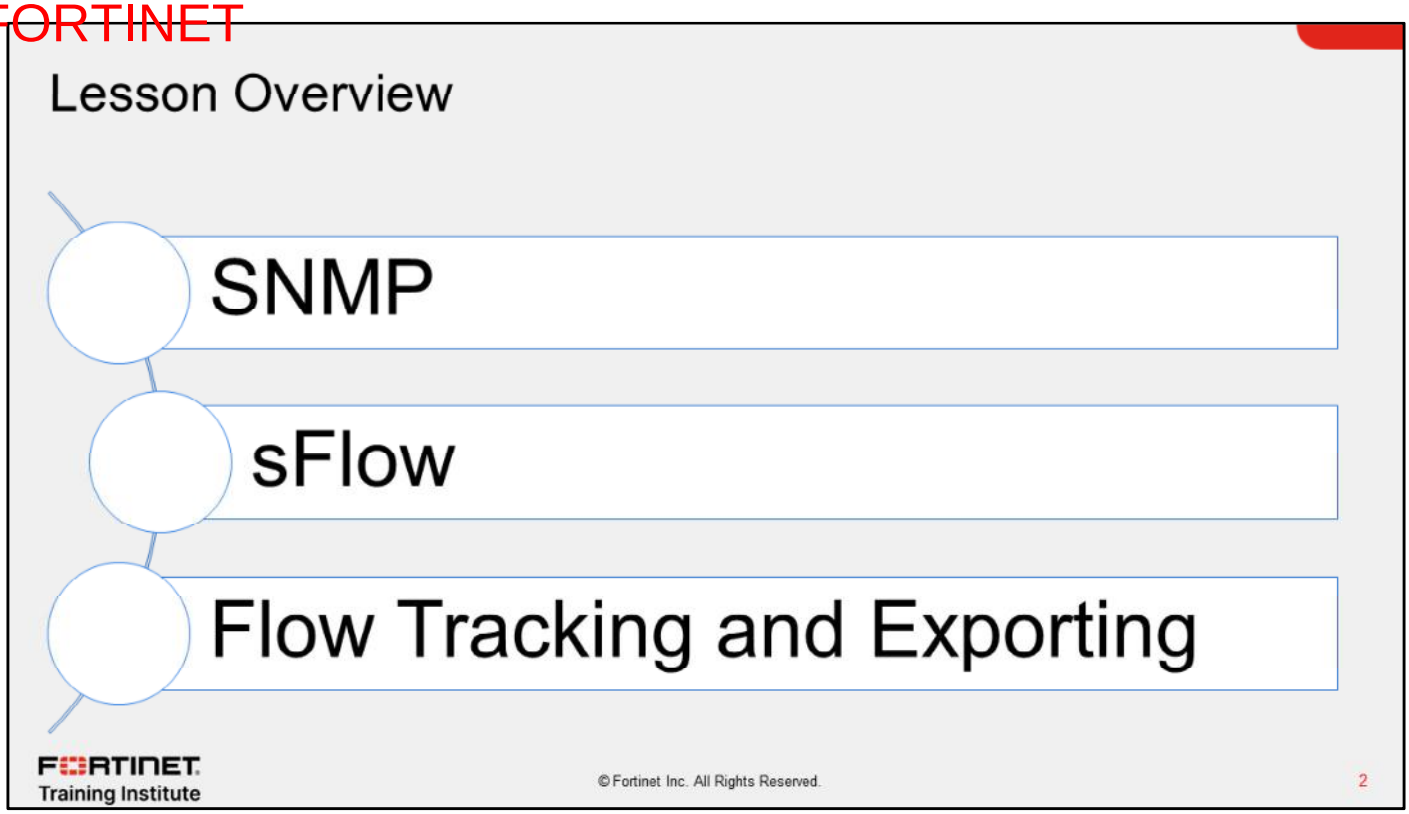
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about some of the monitoring techniques available on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

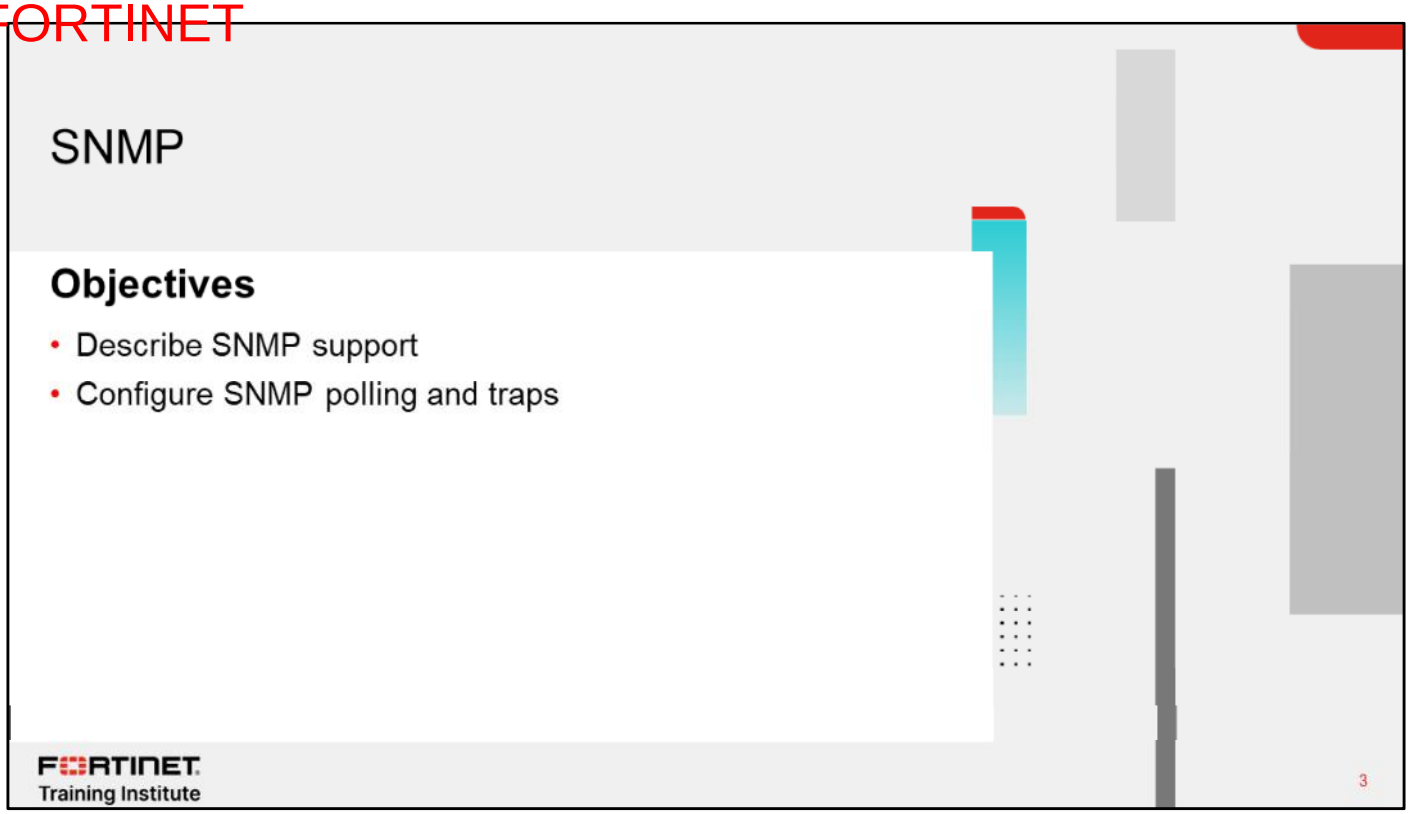
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

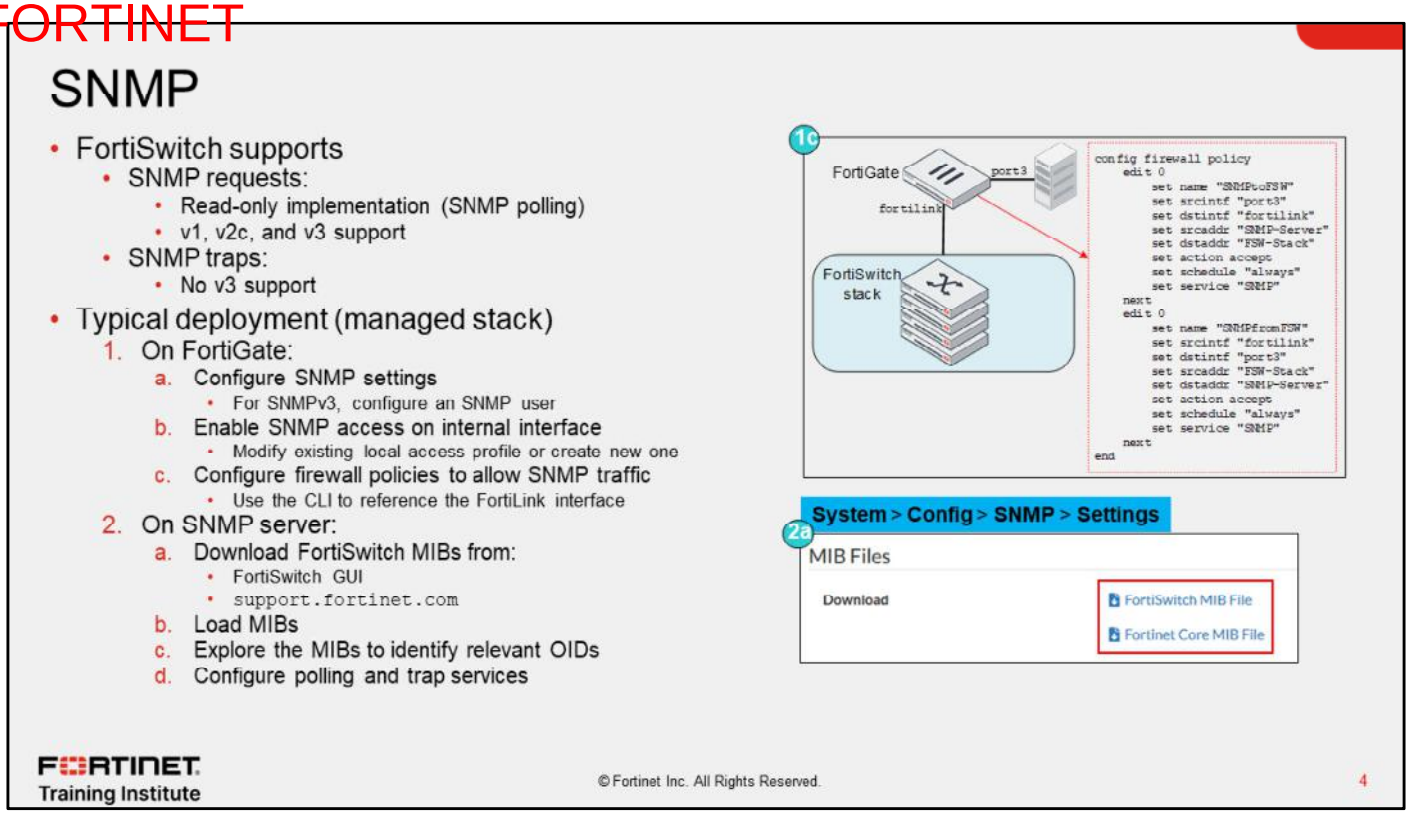


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in SNMP, you will be able to monitor your FortiSwitch stack using the most widely used monitoring protocol.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSwitch supports SNMP versions 1, 2c, and 3. Both SNMP requests and traps are supported. However, for traps, only v1 and v2c are supported. For SNMP requests, implementation is read-only, meaning that you can poll information from FortiSwitch through SNMP only.

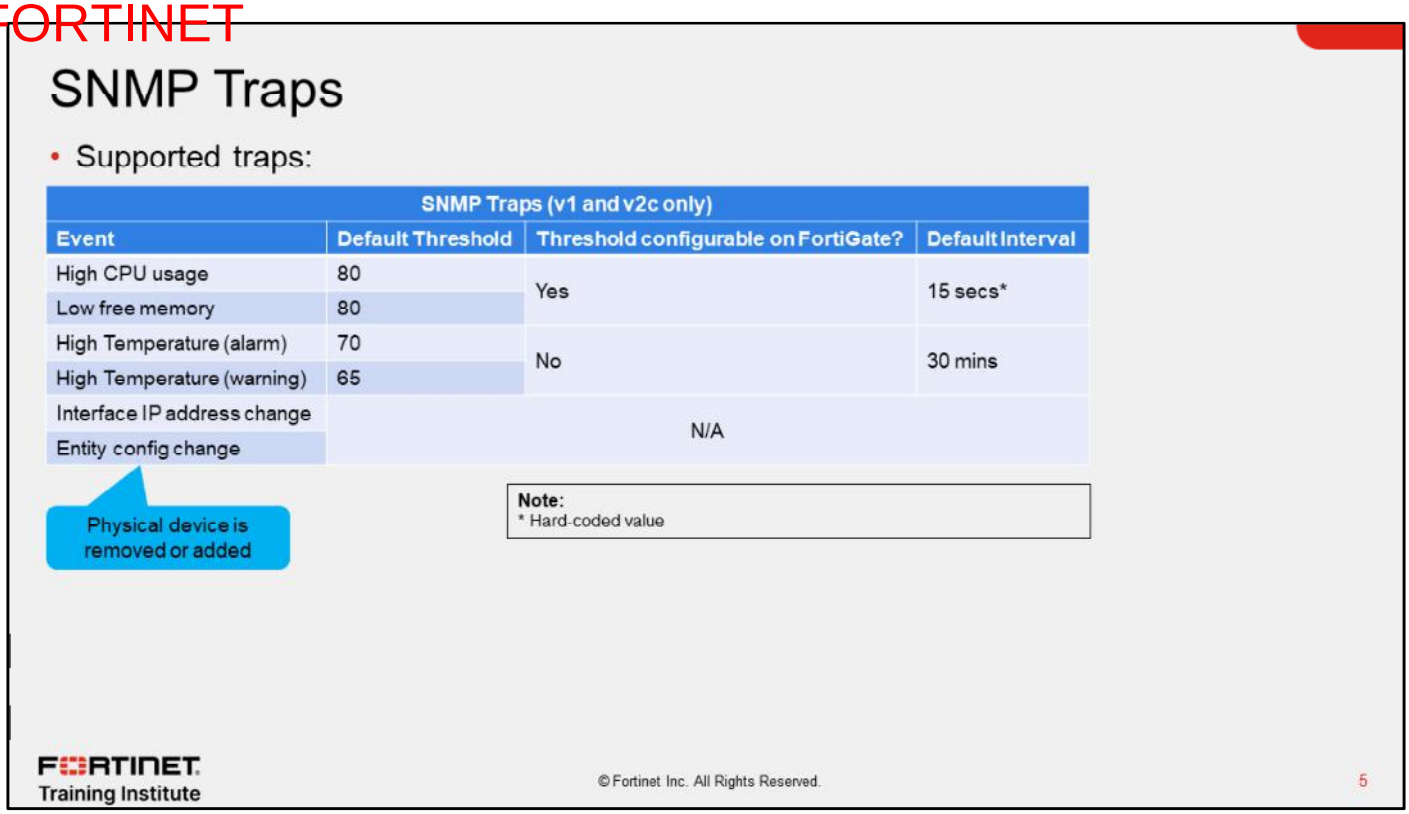
A typical SNMP setup for a managed FortiSwitch stack involves the following steps:

1. On FortiGate:
   a. Configure SNMP settings for FortiSwitch. If you want to use SNMPv3, make sure to configure at least one SNMP user for SNMPv3 authentication and encryption purposes.
   b. Enable SNMP access on the FortiSwitch internal interface. You can either modify the local access profile in use or create a new one.
   c. Configure firewall policies to allow incoming SNMP requests and outgoing SNMP traps. You must use the FortiGate CLI because you must reference the FortiLink interface in the configuration, and the FortiLink interface is not displayed on the FortiGate GUI. This slide shows an example of the firewall policies required on FortiGate to allow SNMP requests and traps from the switch stack.

2. On the SNMP server:
   a. Download the FortiSwitch MIBs from the FortiSwitch GUI or `support.fortinet.com`. This slide shows a screenshot of the FortiSwitch GUI page where you can download the MIBs.
   b. Load the FortiSwitch MIBs to your SNMP server.
   c. Explore the management information base (MIB) files to identify the object identifiers (OIDs) you want to monitor.
   d. Configure polling and trap services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

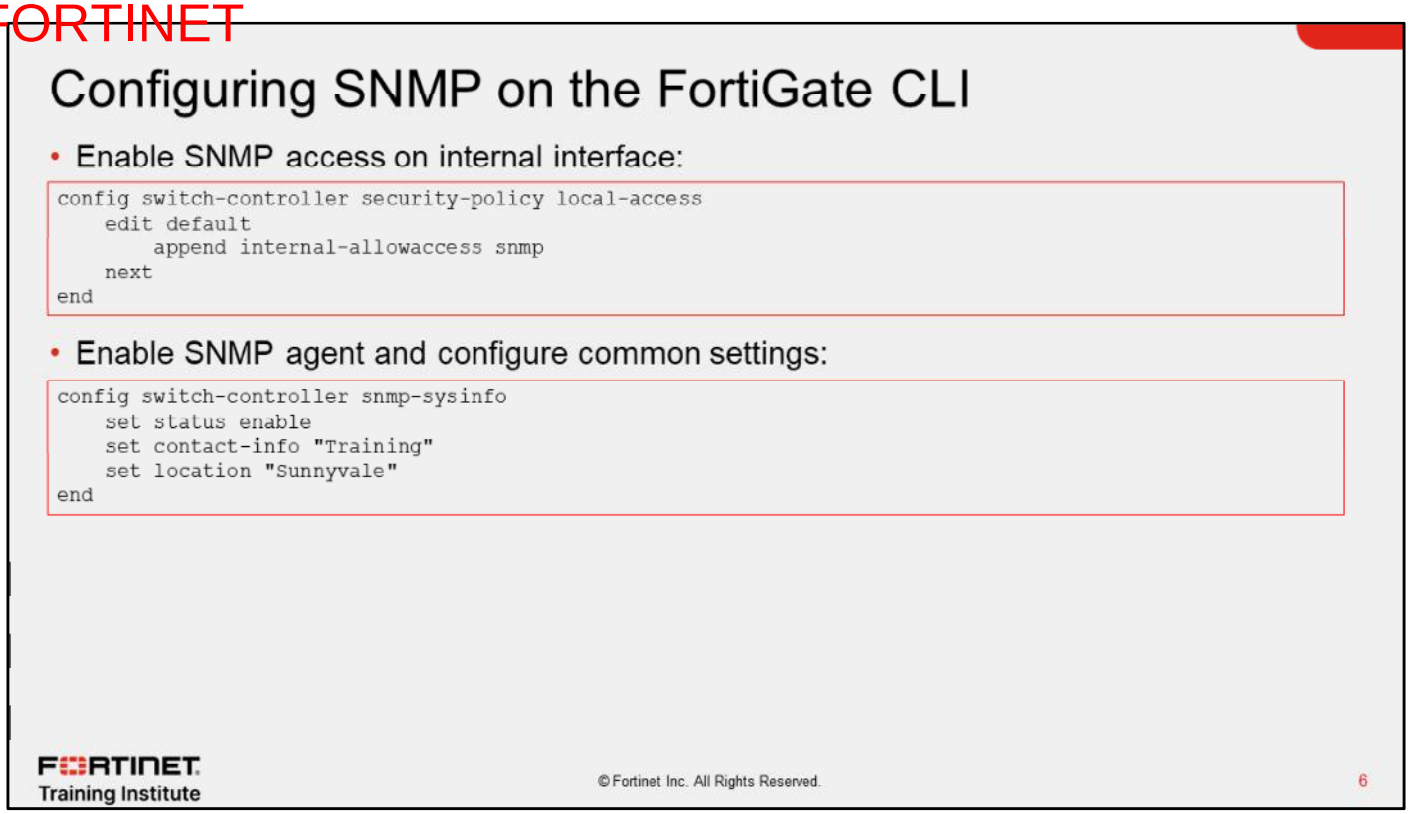


The table on this slide lists the different SNMP traps supported by FortiSwitch. FortiSwitch sends CPU and memory traps at a hard-coded 15-second interval when the configured threshold is exceeded. The temperature traps, however, are sent at a 30-minute interval by default. You can configure the threshold of the CPU and memory traps on FortiGate, but the threshold of the temperature traps must be configured directly on FortiSwitch.

FortiSwitch also sends traps when there is an interface IP address change, or when a physical device is removed from or inserted in the switch. For example, if a PSU is removed or added, an entity config change trap is sent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



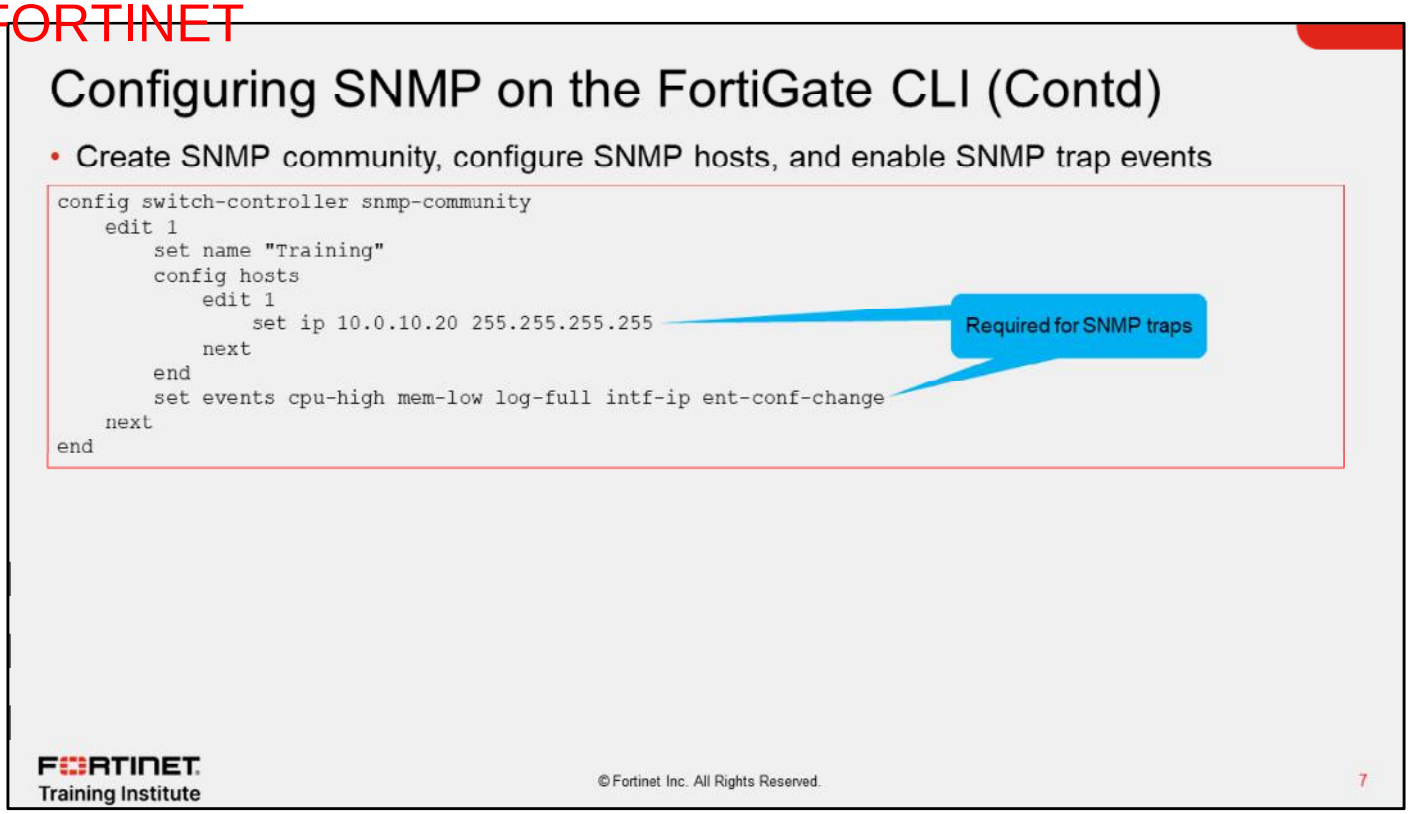
FortiSwitch follows the same SNMP configuration approach as FortiOS. So, if you are familiar with SNMP configuration on FortiOS, then you likely know how to configure SNMP for your managed switches.

You configure SNMP for your managed switches using the FortiGate CLI, as shown on this slide. The first step is to enable SNMP access on the internal interface by either changing the default local access profile or creating a new one. The example shown on this slide changes the default local access profile.

The second step is to enable the SNMP agent and configure the SNMP common settings, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

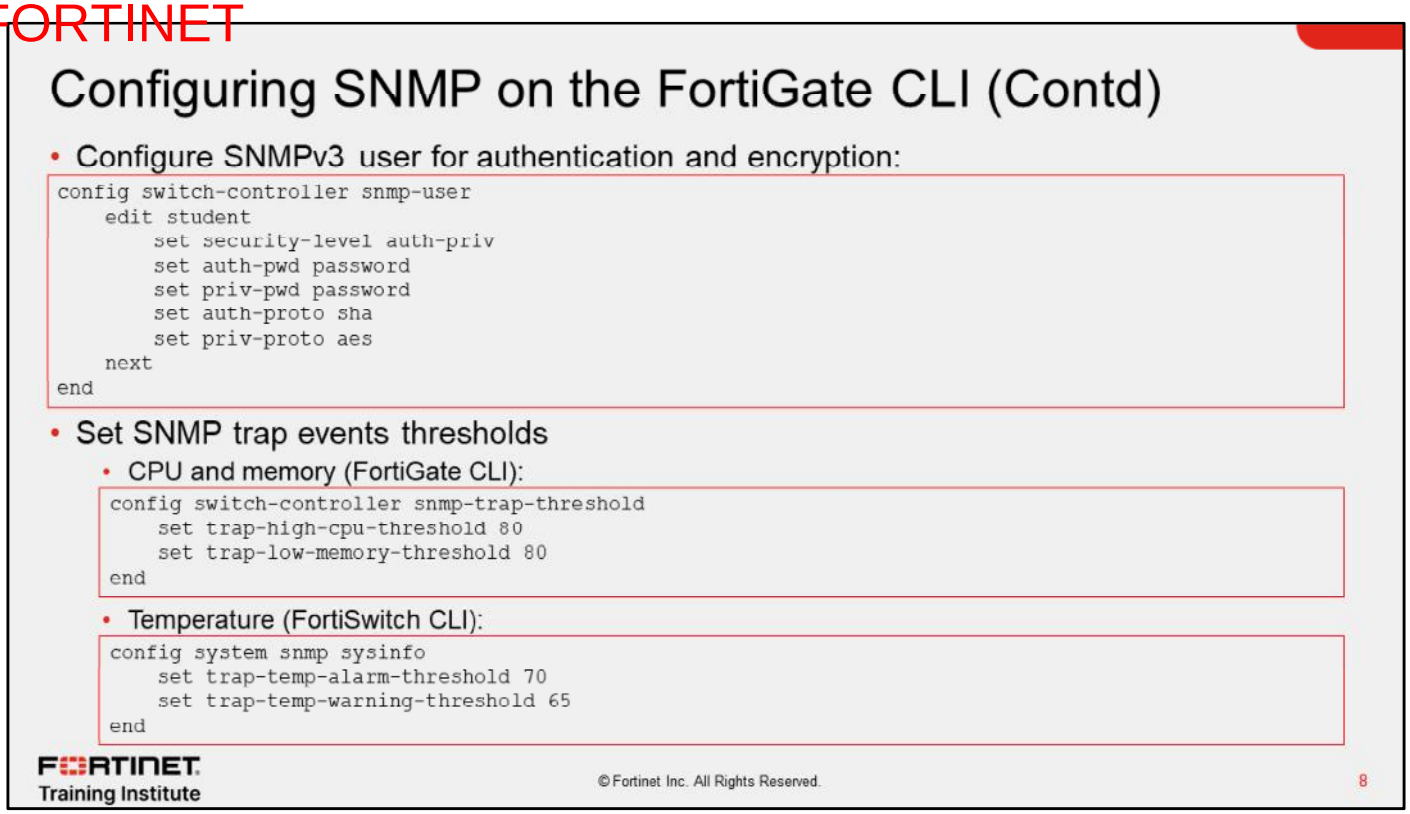
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you enable the SNMP agent and configure SNMP common settings, you must create one or more SNMP communities. The example on this slide shows the configuration for the `Training` community. If you plan to use SNMP traps, make sure you configure at least one SNMP host to send traps to, and select one or more SNMP events to monitor. SNMP hosts also define the source IP addresses where SNMP requests are accepted from. If no SNMP hosts are configured, FortiSwitch accepts SNMP requests from any source, but won't send any SNMP traps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

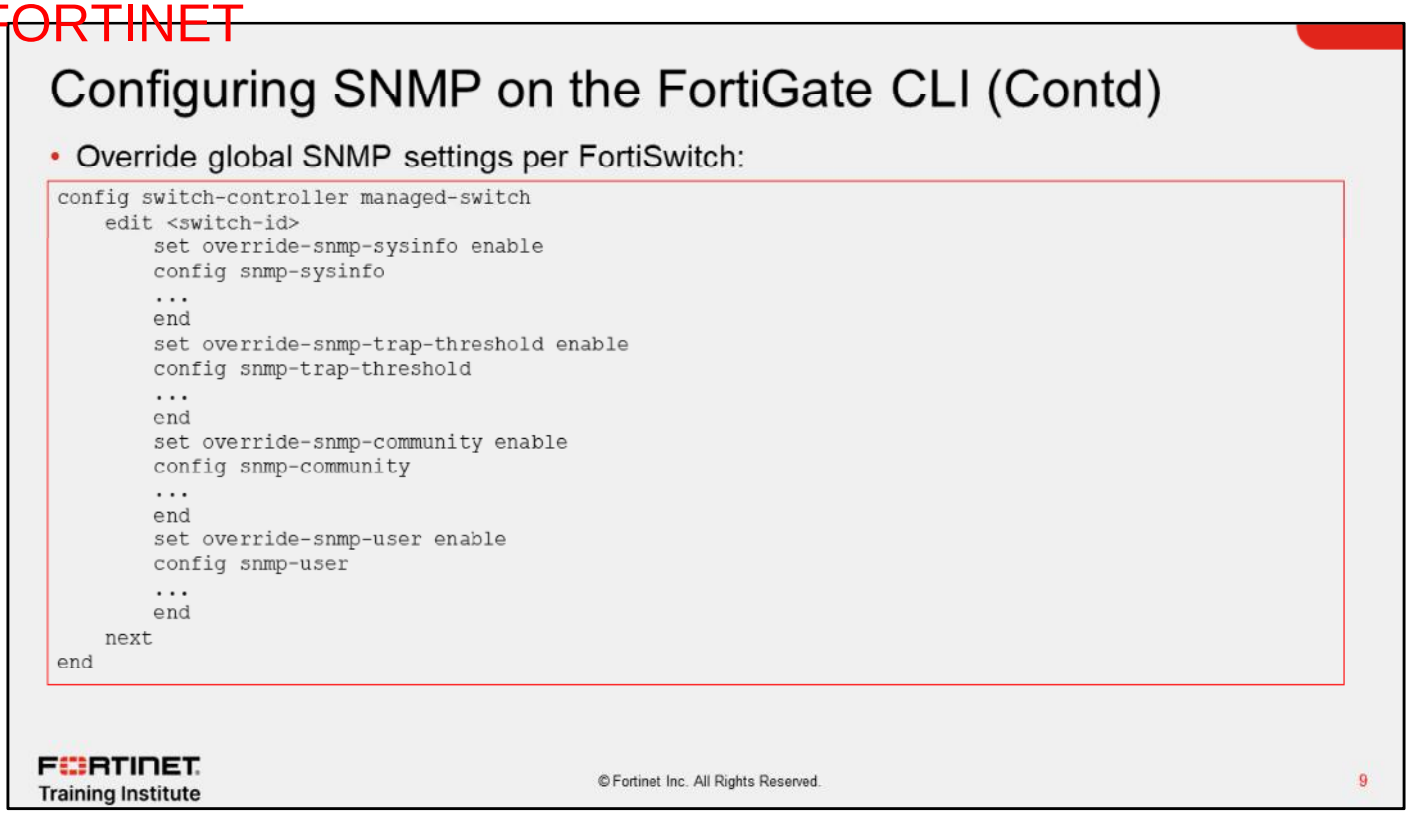


For SNMPv3 requests to work on FortiSwitch, you must configure an SNMP user that defines the security settings to use for authentication and encryption during SNMPv3 requests. The example on this slide shows the configuration for the `student` SNMP user. Note that the configured authentication and encryption (or privacy) protocols are `sha` and `aes`, respectively.

You may also want to change the default thresholds for CPU, memory, and temperature events. Note that you can set new thresholds for CPU and memory on the FortiGate CLI. However, for temperature, you need to set the thresholds directly on the FortiSwitch CLI. Note that FortiSwitch supports SNMP traps for SNMP versions 1 and 2c only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also override the global SNMP settings per FortiSwitch, as shown on this slide. You first indicate the SNMP configuration to override, and then configure the local settings to apply on the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about SNMP in managed switches is true?
   A. SNMPv3 traps are supported.
   ✓B. Firewall policies are required to allow SNMP traffic to and from FortiSwitch.

2. Which setting is required for SNMPv3 to work on FortiSwitch?
   ✓A. SNMP user
   B. SNMP host

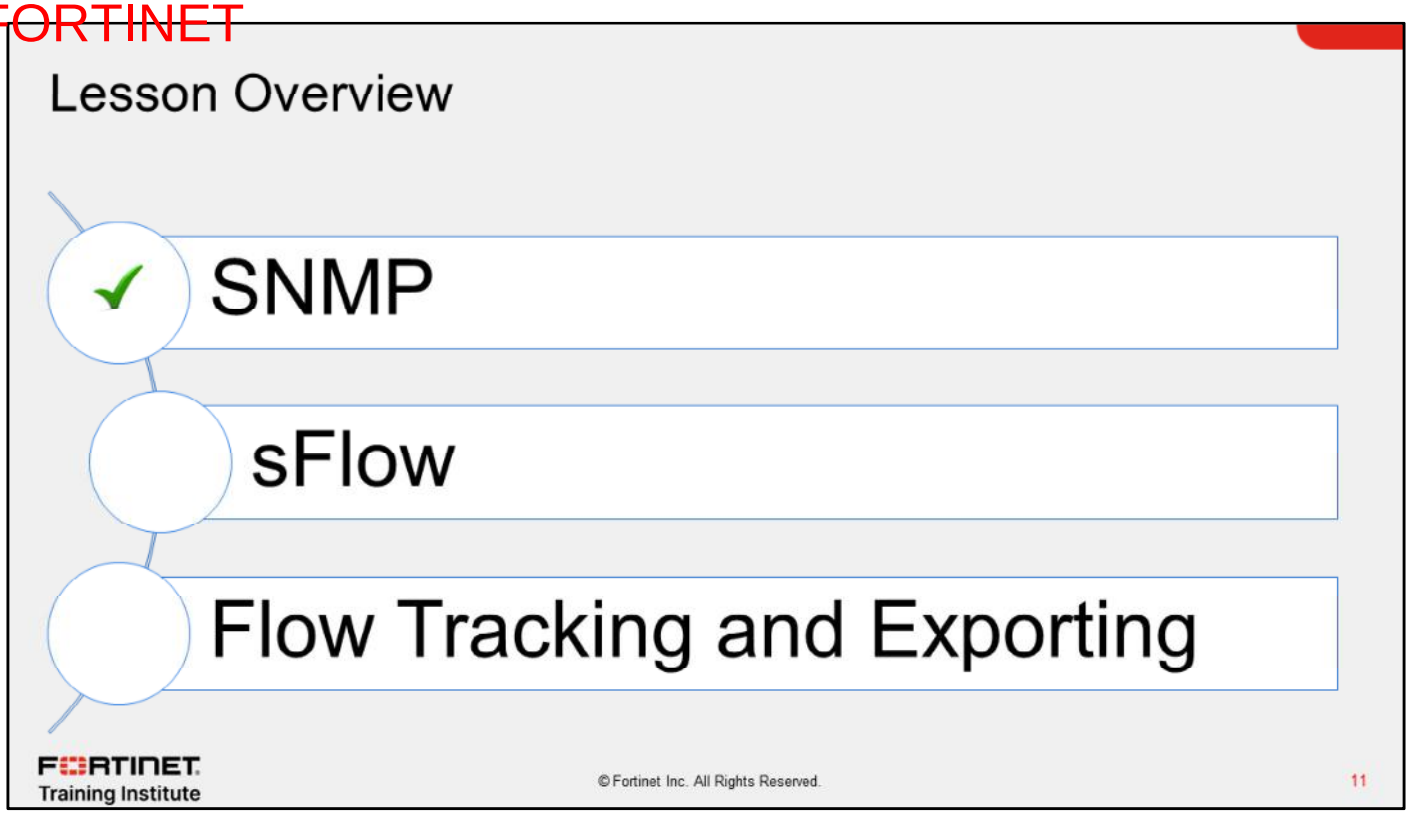
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

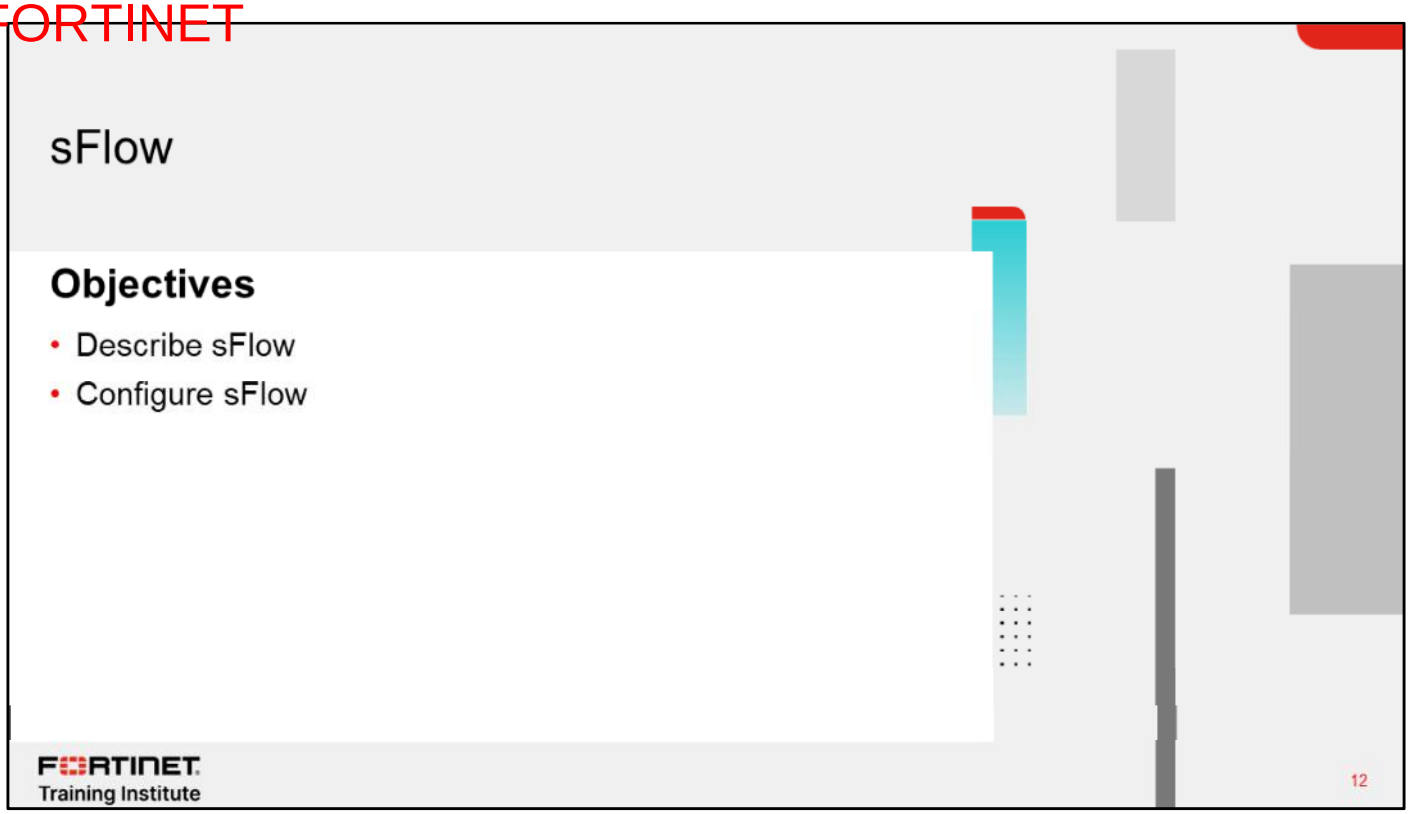


Good job! You now understand SNMP.

Now, you will learn about sFlow.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

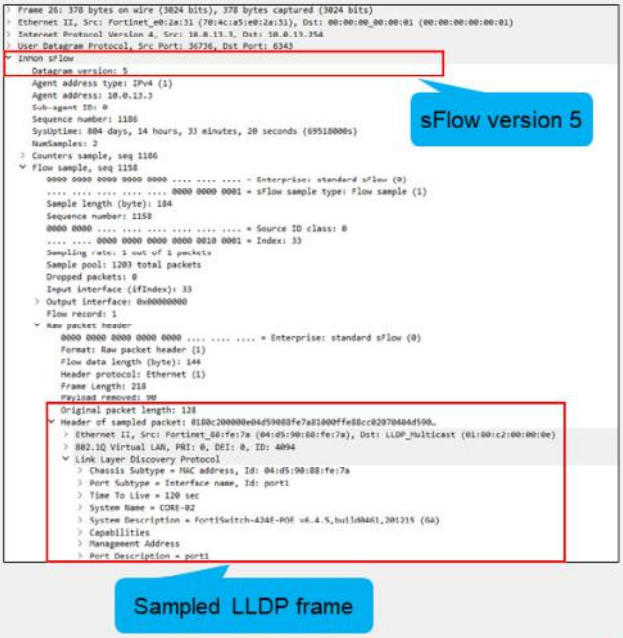
By demonstrating competence in sFlow, you should be able to understand how FortiSwitch can provide more details about the traffic passing through your network by performing packet sampling.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

sFlow

- Alternative method to SNMP
  - Random packets are sampled (packet sampling)
  - Interface counters are sent periodically (counter sampling)
  - Supported version: 5
- When compared to SNMP, sFlow:
  - Is more CPU intensive
  - Provides traffic details in addition to interface stats
- Alternative to SPAN, RSPAN, and ERSPAN
  - Can be used on trunks
- Typical deployment (managed stack)
  1. On FortiGate:
     a. Configure sFlow collector settings
     b. Enable packet sampling on interface and set:
        - Sampling rate
        - Interface counter interval
        - Traffic direction to monitor
     c. Configure firewall policies to allow sFlow datagrams
        - Use the CLI to reference the FortiLink interface as source
  2. On sFlow collector, confirm flows are received



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

Another method available for monitoring traffic passing through the switch is sampled flow (sFlow). When you enable sFlow on a FortiSwitch interface, the switch captures random packets on the interface—known as packet sampling—and then encapsulates the sampled packets in sFlow datagrams that are sent to the configured sFlow collector. FortiSwitch also sends periodic interface counters to the sFlow collector—known as counter sampling. Upon receiving the sFlow data, the collector provides real-time traffic analysis and reports. Note that FortiSwitch supports sFlow version 5.

Because of packet sampling, sFlow is likely to be more CPU intensive than SNMP. However, sFlow provides you with details about the traffic in your network instead of just providing you with the overall traffic statistics, like SNMP does. sFlow is also a troubleshooting alternative to SPAN, RSPAN, and ERSPAN, because you can use sFlow to capture packets received or sent on a switch interface. However, unlike SPAN, RSPAN, and ERSPAN, which can't be used on trunks, sFlow is supported on trunks.

A typical sFlow setup for a managed FortiSwitch stack involves the following steps:

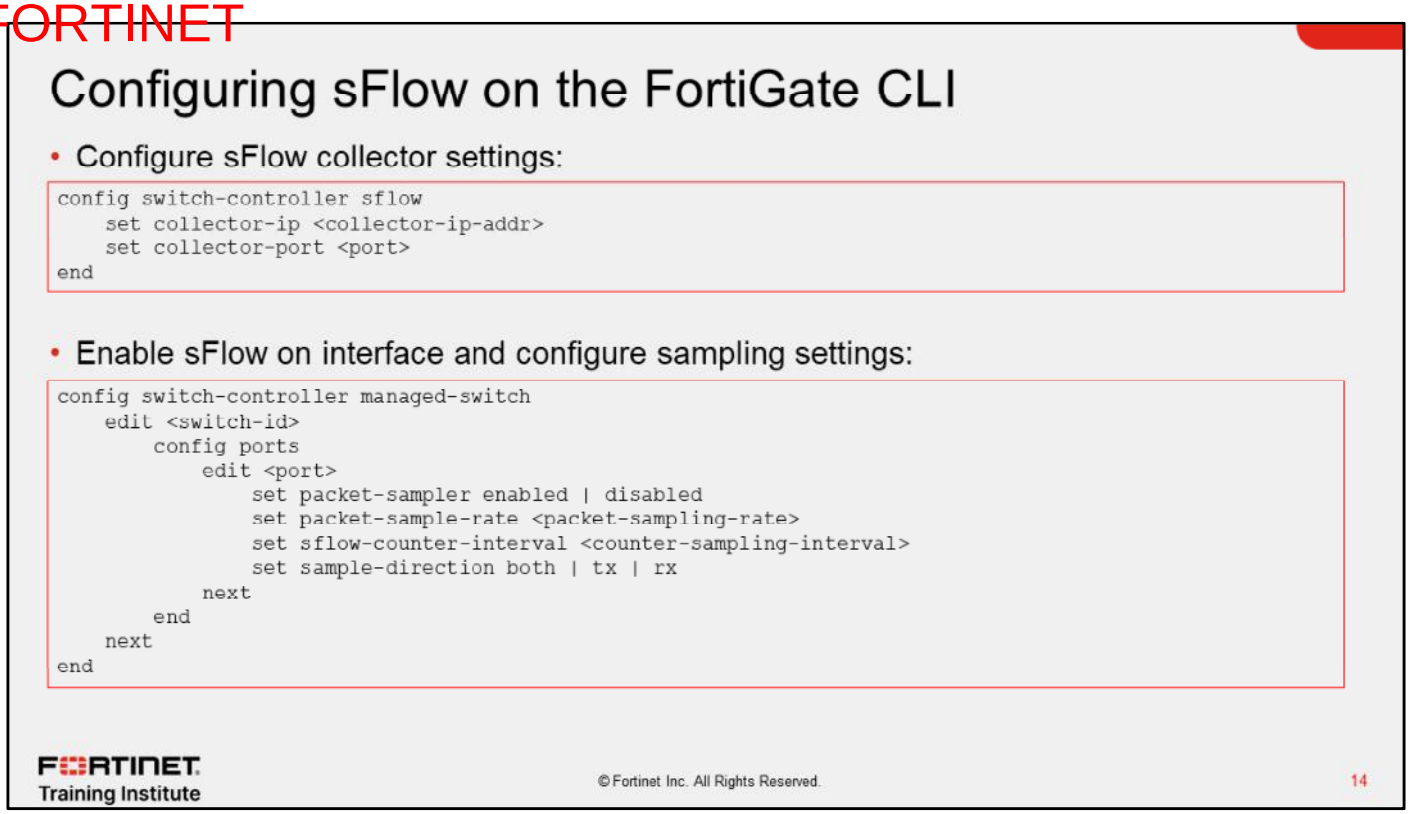
1. On FortiGate:
   a. Configure sFlow collector settings for FortiSwitch.
   b. Enable packet sampling on the FortiSwitch interfaces to monitor, and then set the packet sampling rate, interface counter interval, and the traffic direction to monitor.
   c. Like SNMP, you must also configure firewall policies to allow the sFlow datagrams sent to the collector.

2. On the sFlow collector, confirm that flows are received.

The image on this slide shows an sFlow datagram from FortiSwitch that encapsulates a sampled LLDP frame.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Like SNMP, FortiSwitch follows the same sFlow configuration approach as FortiOS.

You configure sFlow for your managed switches using the FortiGate CLI, as shown on this slide. The first step is to configure the sFlow collector IP address and port. The default port is `6343`.

The second step is to enable sFlow on the switch interface and then configure the corresponding sFlow sampling settings:

- Packet sampling rate: This is set to `512` by default. That is, 1 in 512 packets are sampled. The lower the sampling rate, the higher the CPU usage. A rate of 512 works most of the time, but you may want to increase the rate on higher-speed interfaces processing large amounts of traffic.
- Counter sampling interval: This defines the interval for the counter sampling. It's set to `0` by default, which means that periodic interface counters are not sent. If you want your sFlow collector to accurately track the utilization on a port, then it is recommended to set the interval between 20 to 30 seconds.
- Sampling direction: This defines whether you want to enable sFlow for both directions of the traffic, or for the transmit or receive directions only. It's set to `both` by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about sFlow is true?

✓A. sFlow can perform packet sampling and counter sampling.
B. sFlow is less CPU intensive than SNMP.

2. What is the `sflow-counter-interval` setting used for?

A. It defines the interval at which packets are sampled.
✓B. It defines the interval at which interface counters are sent.

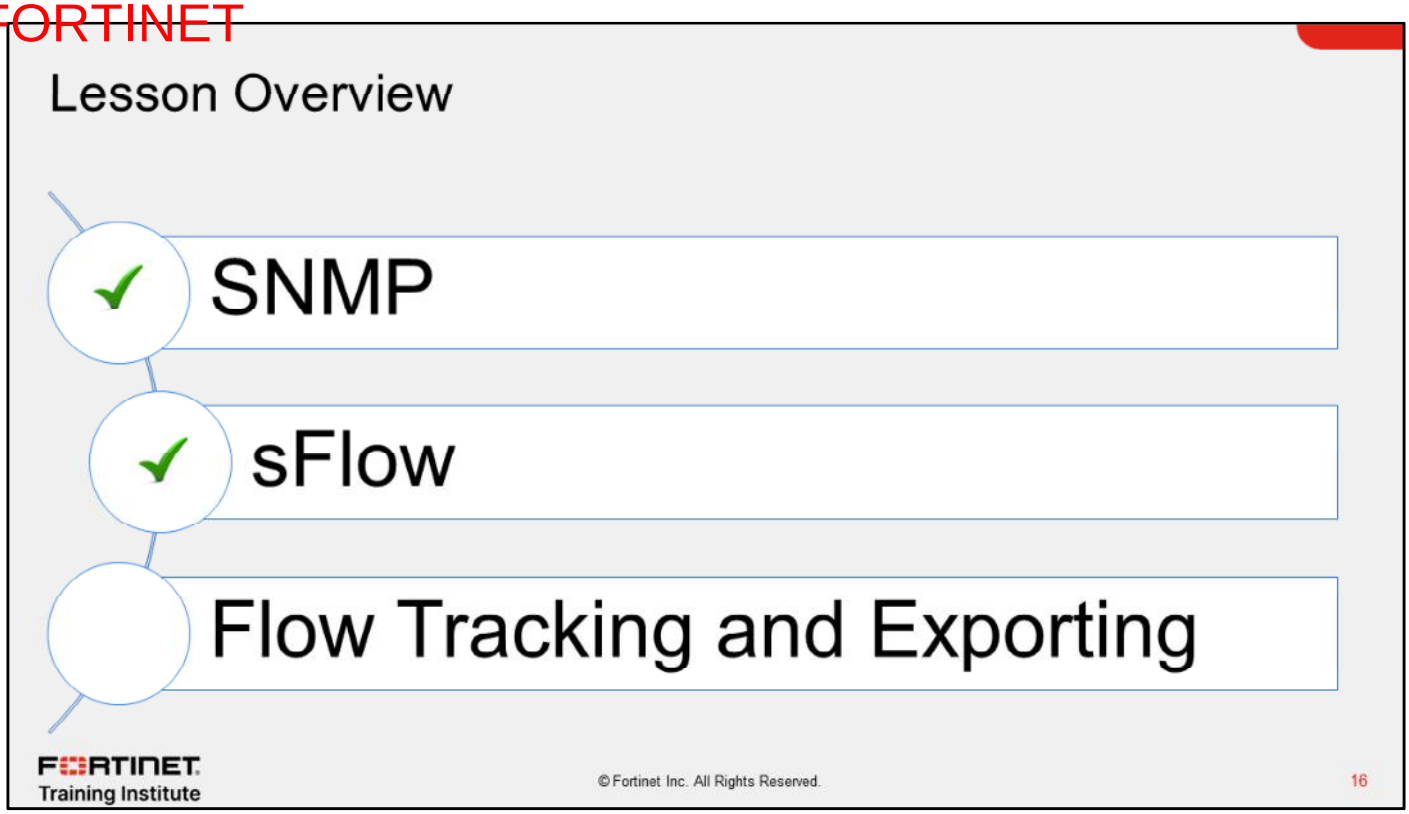
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand sFlow.

Now, you will learn about flow tracking and exporting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

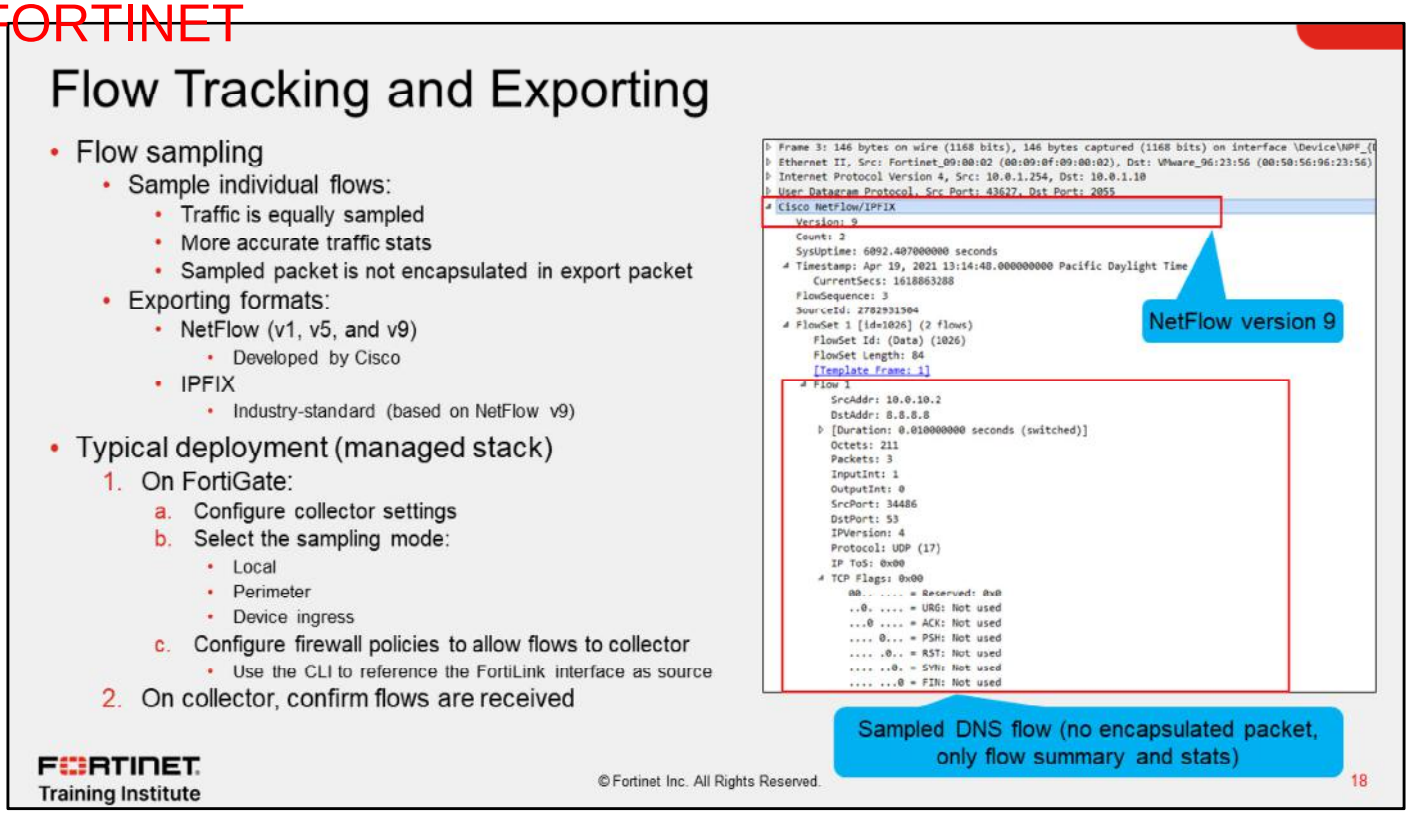


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in flow tracking and exporting, you should be able to understand how FortiSwitch can perform flow sampling and export the sampled flows to a collector using NetFlow or IPFIX formats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSwitch can also track individual flows and export their information to a collector using different formats. Unlike sFlow, which samples packets received or transmitted on a port (packet sampling), flow tracking samples packets on individual flows (flow sampling). Flow sampling is more accurate than packet sampling because all flows are sampled equally whereas, with packet sampling, bursty flows are sampled at a higher rate than non-bursty flows, which leads to less accurate traffic statistics. One downside of using flow sampling is that it does not encapsulate sampled packets in the flows sent to the collector, like sFlow does. This prevents flow sampling from being used as a packet capture alternative.

When you enable flow tracking and exporting, you also export information for sampled flows using NetFlow or Protocol Flow Information Export (IPFIX) formats. NetFlow was developed by Cisco, and FortiSwitch supports versions 1, 5, and 9. IPFIX is the industry-standard version of NetFlow and is based on NetFlow version 9.

A typical flow tracking and exporting setup for a managed FortiSwitch stack involves the following steps:

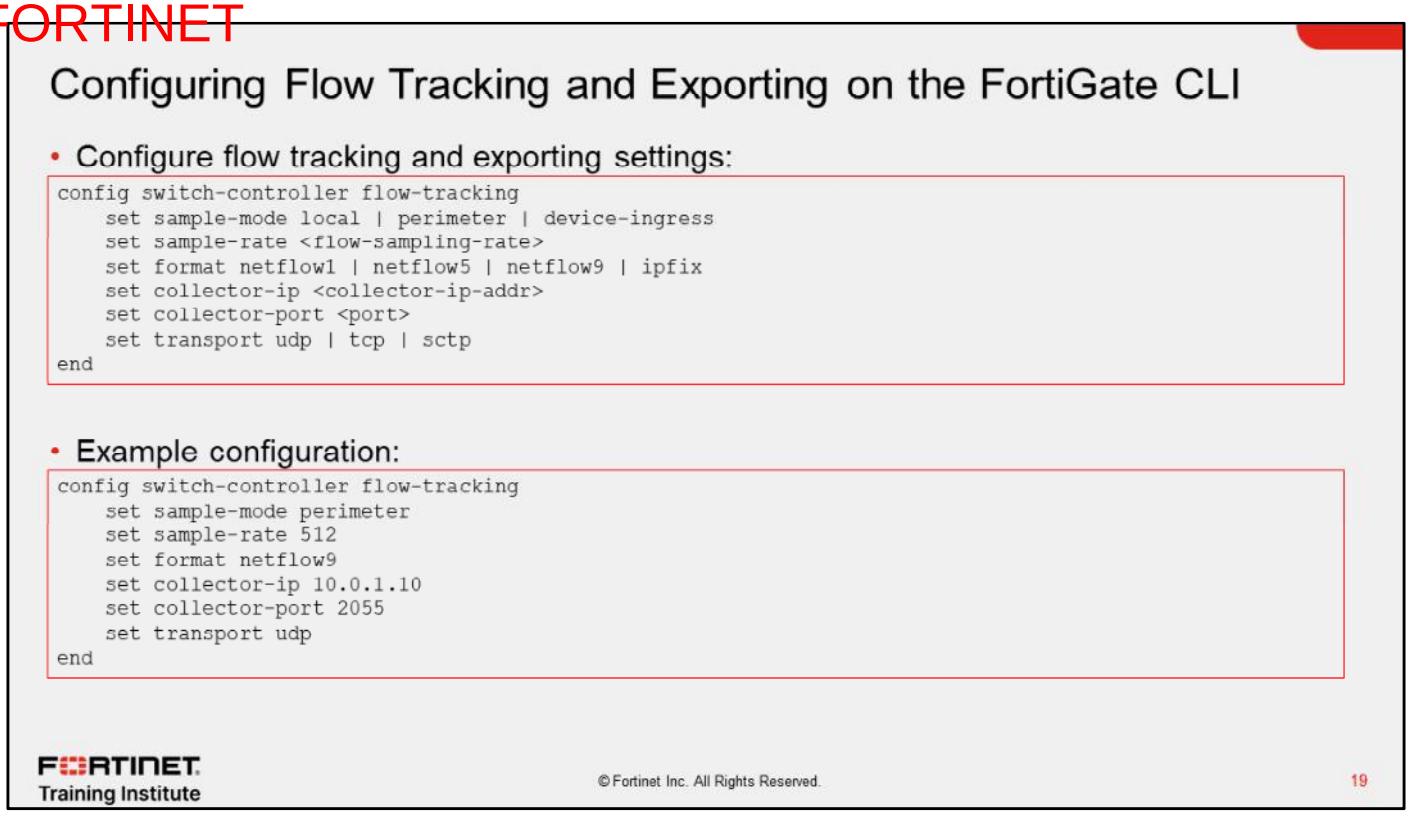
1. On FortiGate:
   a. Configure collector settings for FortiSwitch.
   b. Select one of the supported sampling modes: local, perimeter, or device ingress.
   c. Configure firewall policies to allow NetFlow or IPFIX flows to the collector.

2. On the collector, confirm that flows are received.

The image on this slide shows a NetFlow version 9 packet from FortiSwitch that contains information about a sampled DNS flow. Note that only a summary of the network connection for the flow is provided, and that there are no encapsulated packets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



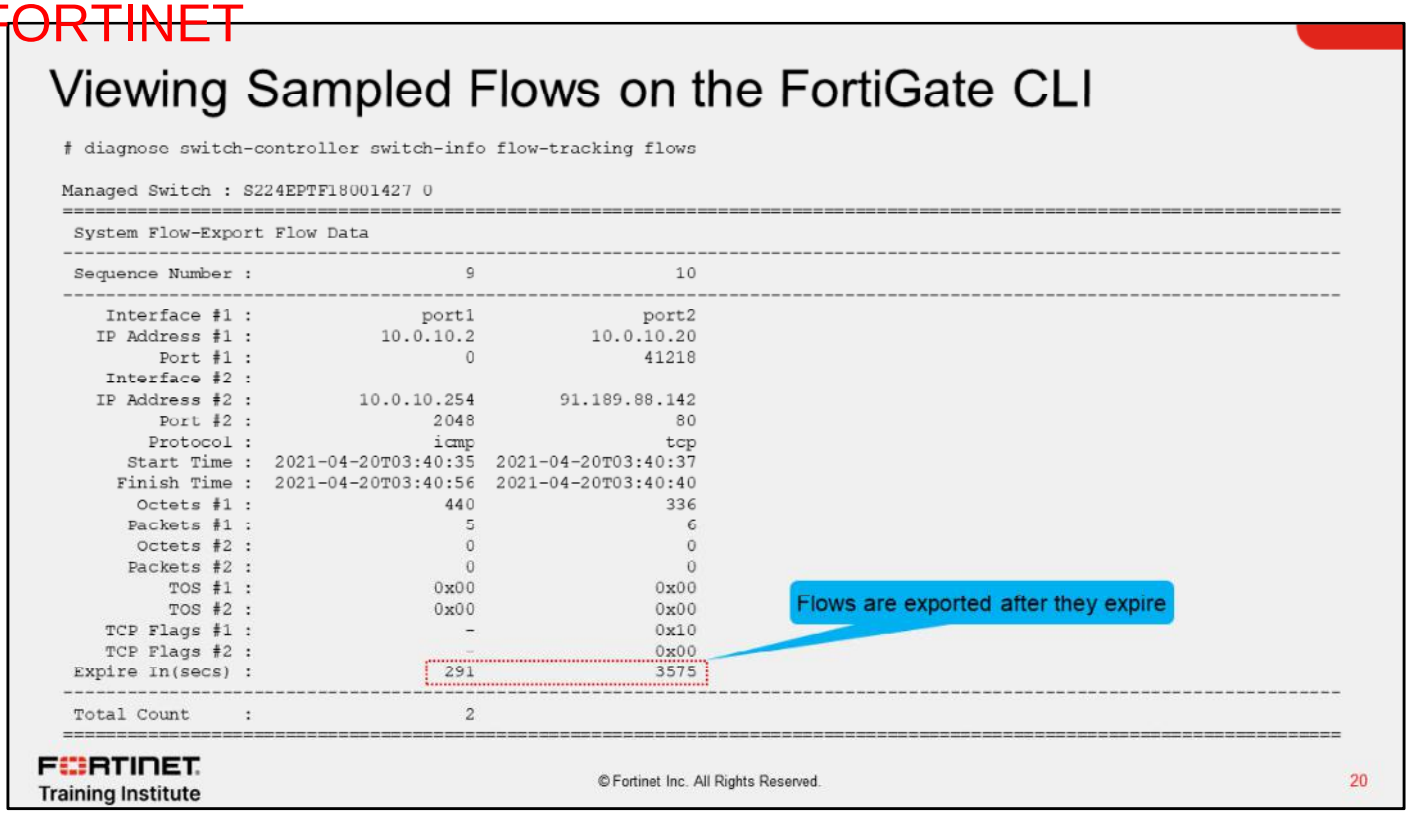
When you configure flow tracking and exporting on your managed FortiSwitch stack, all the configuration is done under `config switch-controller flow-tracking`.

- In sampling mode, the following options are available:
  - `local`: FortiGate turns on flow sampling on FortiSwitch but doesn't change existing sampling settings of interfaces. It is up to the administrator to configure the following port-level sampling settings: `packet-sampler`, `packet-sample-rate`, and `sample-direction`.
  - `perimeter`: FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces, except ICL and ISL interfaces. Traffic entering the FortiLink trunk is also sampled. The goal is to sample traffic entering the FortiSwitch stack perimeter. Think of the FortiSwitch stack perimeter as the switch ports where endpoints, including FortiGate, are connected.
  - `device-ingress`: FortiGate configures FortiSwitch to perform ingress sampling on all switch interfaces. The goal is to sample all the traffic across the FortiSwitch stack. This is, both north-south and east-west traffic.
- Packet sampling rate: Serves the same purpose as sFlow, except that the rate applies to *individual* flows, and not to all the traffic on a port, like in the sFlow case.
- Format: Choose between NetFlow v1, v2, and v9, and IPFIX.
- Collector IP: Set the IP address of the collector. FortiSwitch starts performing flow sampling only after you set the collector IP address. Set the IP to `0.0.0.0` to turn off flow sampling.
- Collector port: Set the port the collector is listening on for NetFlow and IPFIX flows. Usually, collectors listen on port 2055.
- Transport: Set the transport protocol used for flows. Usually, UDP works for most deployments.

This slide shows the most common settings that administrators adjust. For a full list of available settings, refer to the *FortiSwitch—Managed by FortiOS* document on `docs.fortinet.com`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how to display the flows that are currently being sampled by FortiSwitch using the FortiGate CLI. For each flow, common network parameters are shown, such as the source and destination IP address, source and destination ports.

In addition, each flow is assigned an expiration timer. FortiSwitch samples packets for a flow until the flow expires, which is when the flow is exported to the collector. If you want FortiSwitch to export flows to the collector immediately, you can manually expire all flows on FortiSwitch by running the `diagnose sys flow-export expire-flows-all` command on the FortiSwitch CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about flow tracking and exporting is true?
   - A. FortiSwitch performs packet sampling
   - ✓ B. FortiSwitch can export flows using NetFlow and IPFIX formats

2. When does FortiSwitch export a sampled flow to the collector?
   - A. After it samples the first packet of the flow
   - ✓ B. After the sampled flow expires

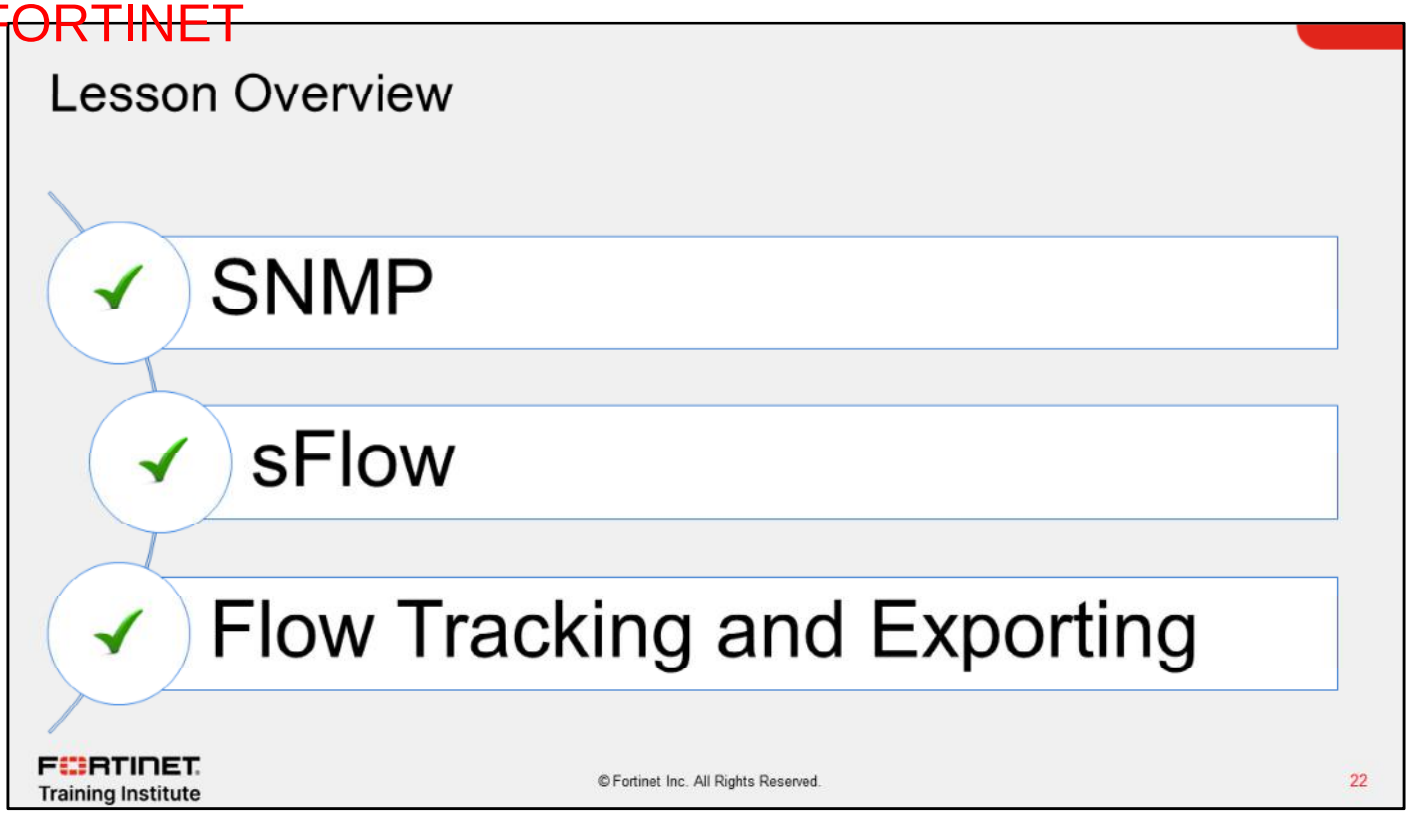
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

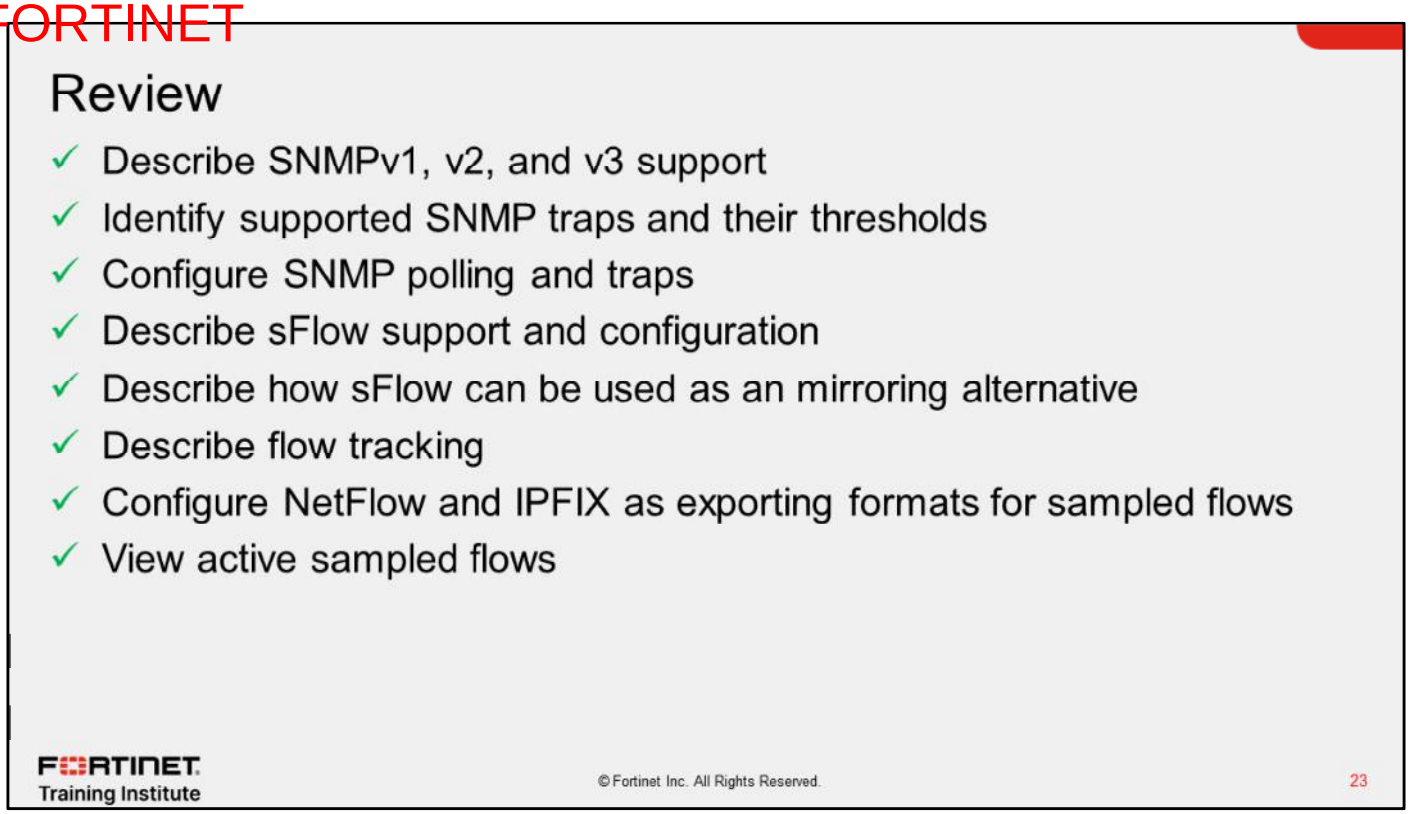


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

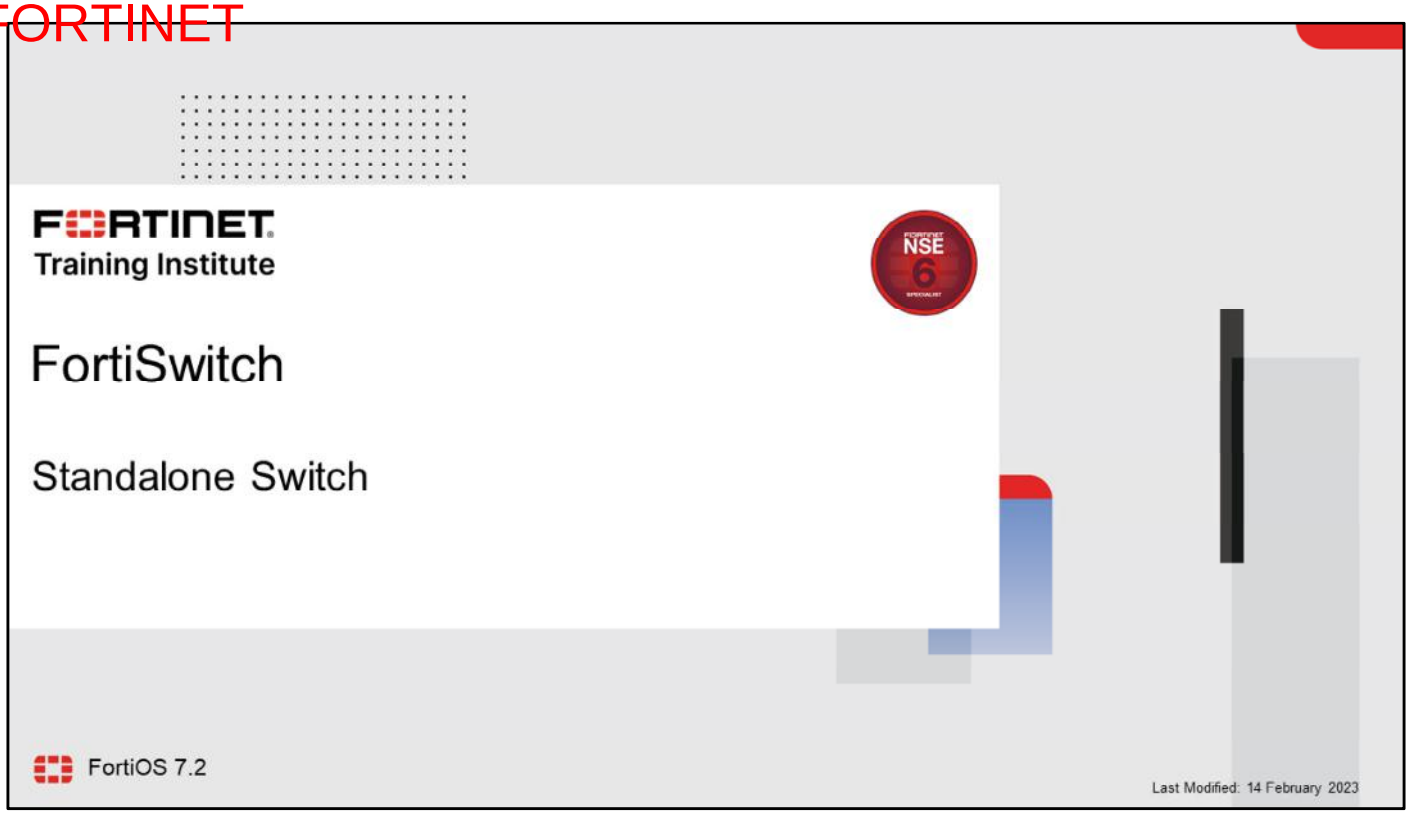


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the different options available on FortiSwitch for monitoring the traffic passing through your managed stack, as well as the health of the switches.

Vouchers & Dumps are Available | WhatsApp +201224560923

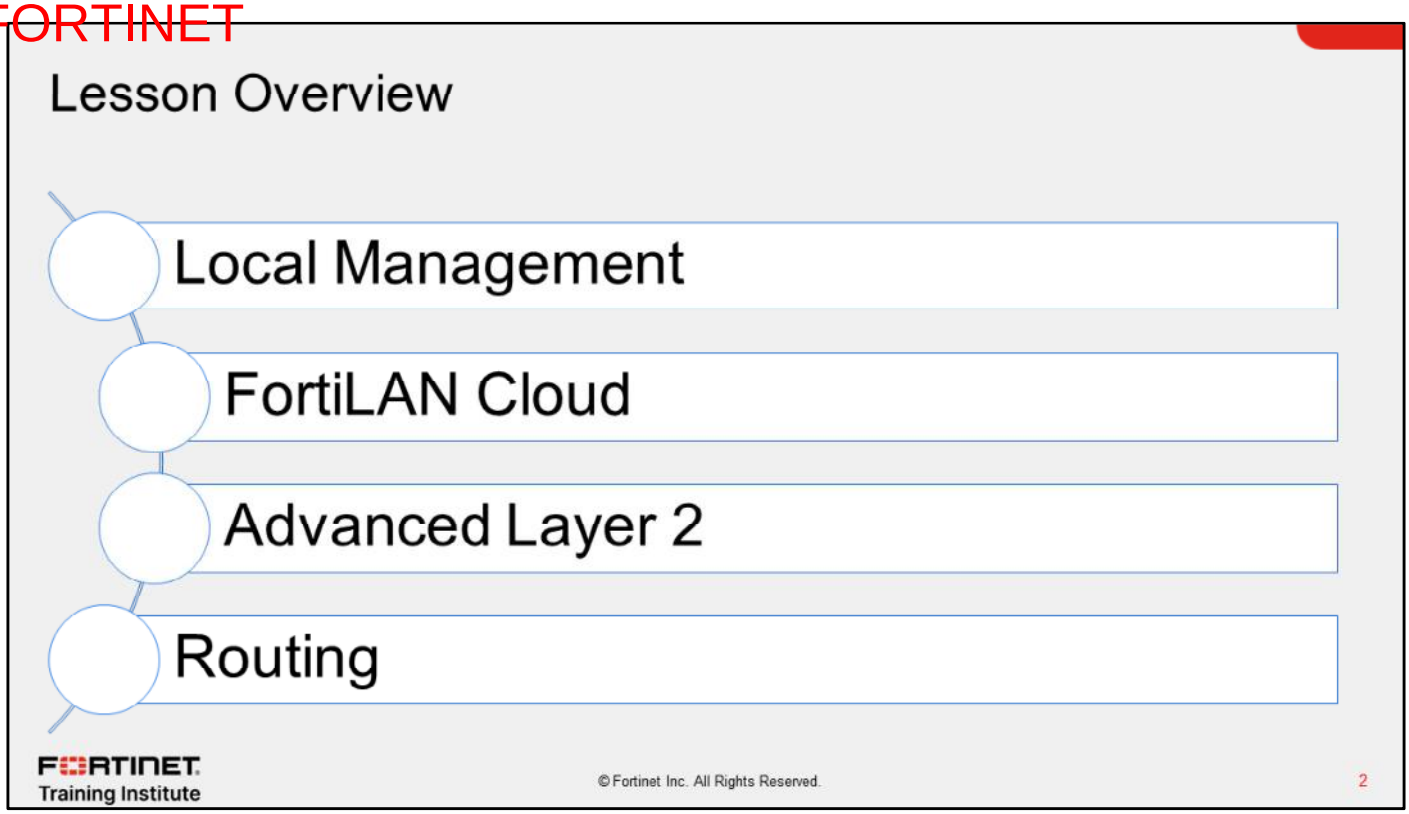
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSwitch standalone management, and some of the unique features available in standalone mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

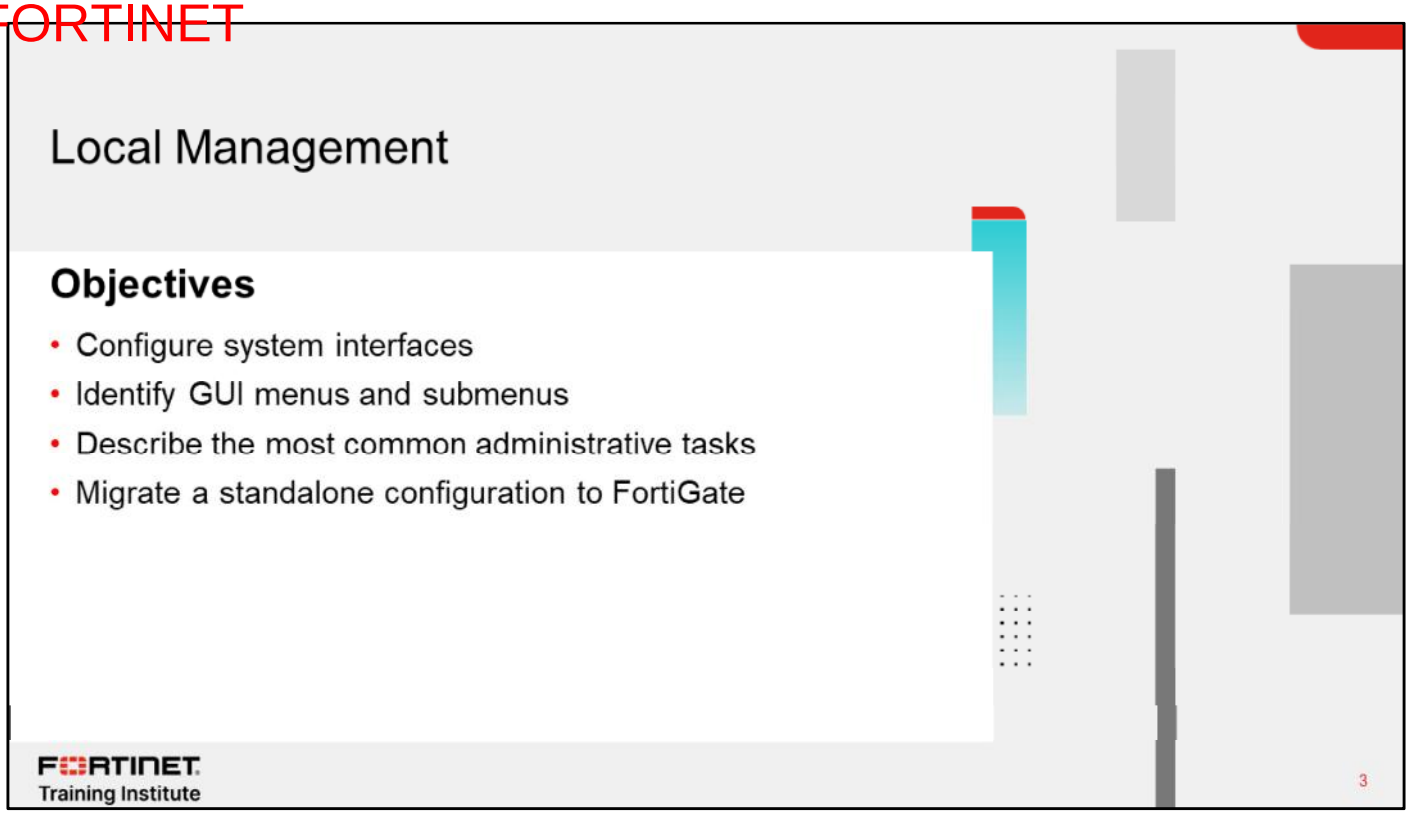
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

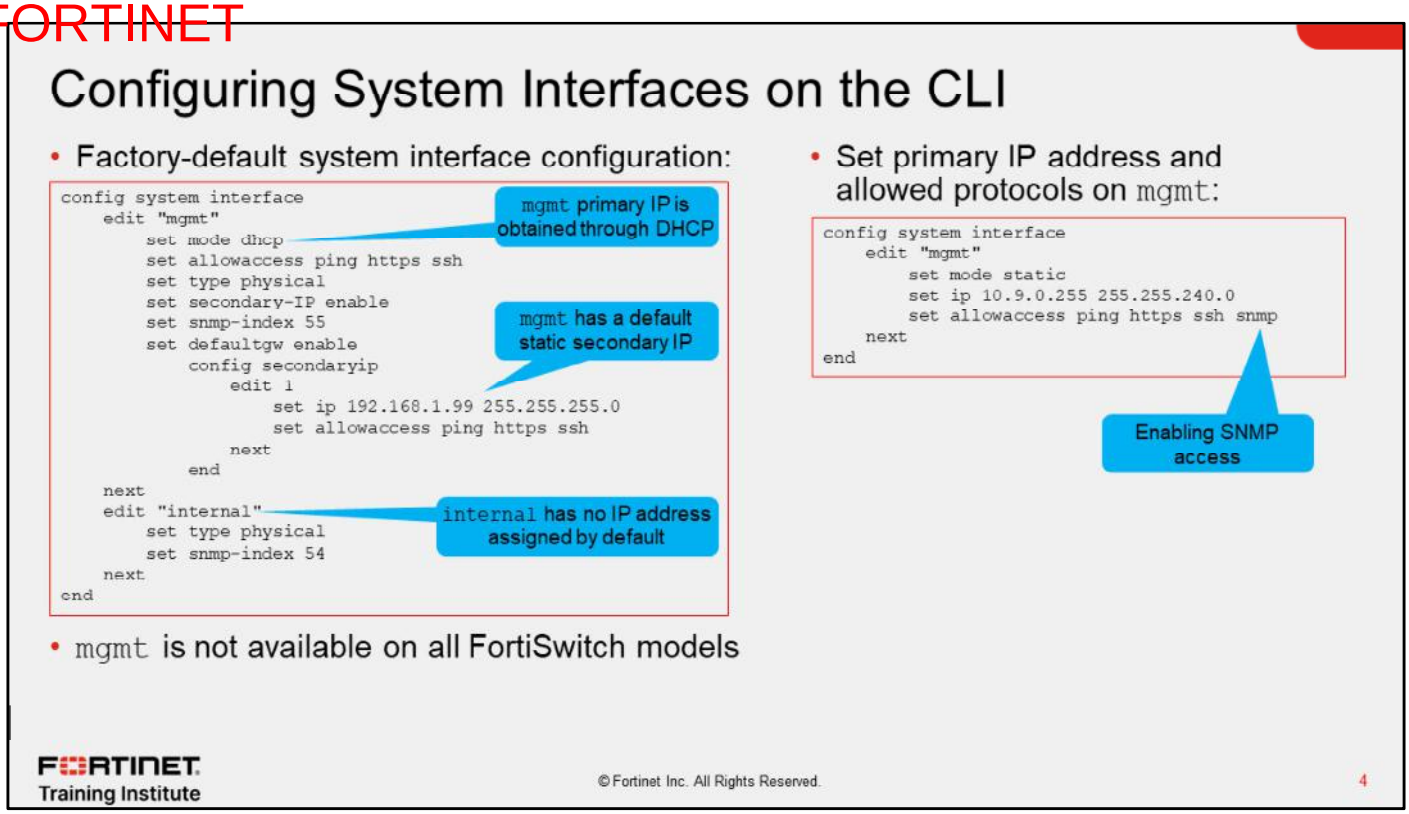


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in local management, you should be able to understand how to configure and monitor FortiSwitch in standalone mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



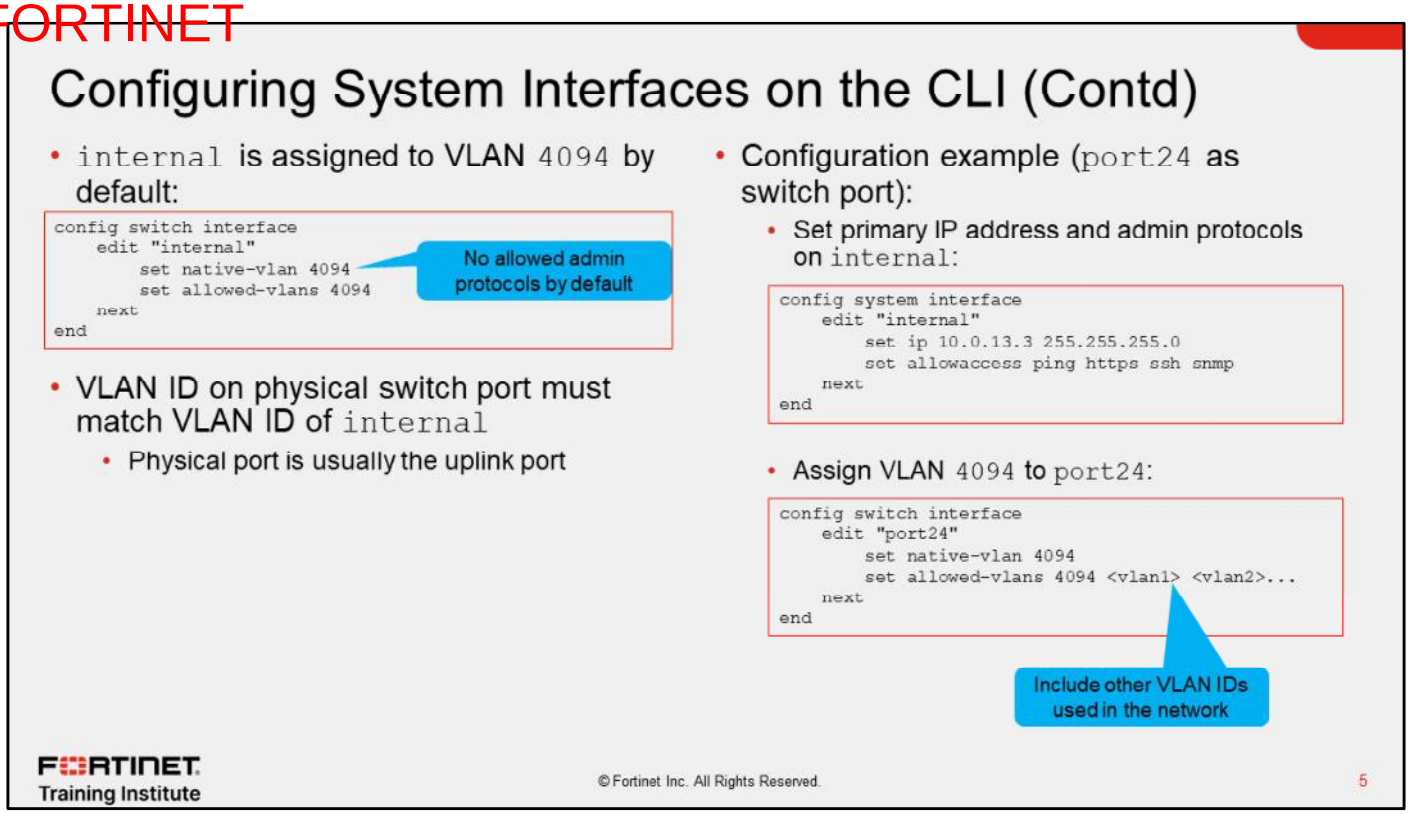
The first configuration change that administrators usually make is to assign a management IP to FortiSwitch using the console port. There are two management interfaces available on FortiSwitch: `mgmt` and `internal`. The `mgmt` interface provides you with out-of-band switch management. The `internal` interface is a logical in-band management interface that is accessed through the switch ports. Note that all FortiSwitch models come with an `internal` interface, but some come with a `mgmt` interface.

This slide shows the factory-default configuration for both interfaces. Note that although the `mgmt` interface is configured to get its primary IP from DHCP, the interface is also assigned the secondary IP `192.168.1.99/24`. This means that you can connect a PC to the `mgmt` port, assign the PC NIC any IP in the `192.168.1.0/24` subnet, and then access the switch from the PC. Alternatively, you can connect `mgmt` to your LAN to get an IP over DHCP, or just assign a different static IP address.

This slide shows how to assign a primary IP address on the `mgmt` interface and how to add SNMP to the list of allowed administrative protocols. By default, `mgmt` allows PING, HTTPS, and SSH protocols only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

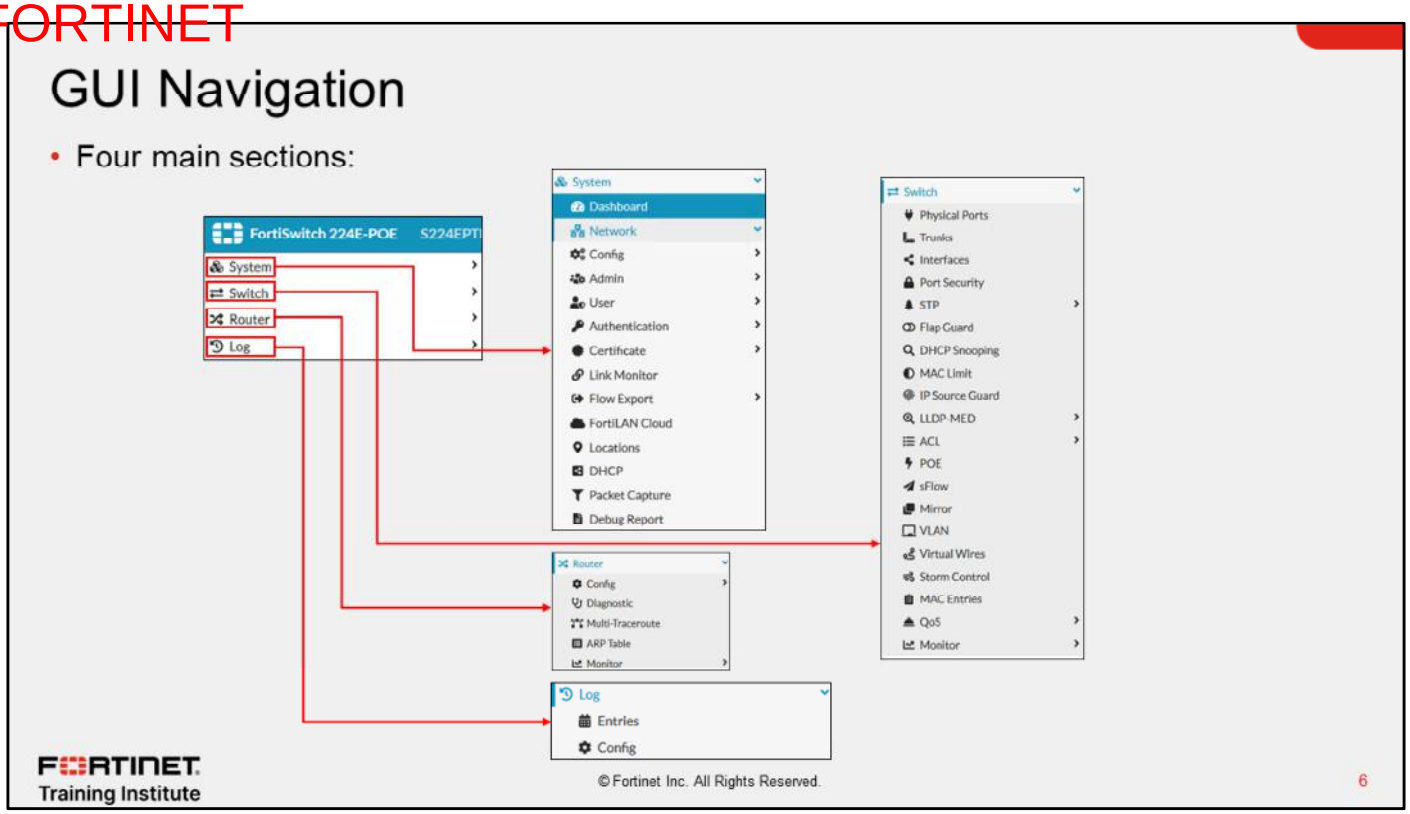


The `internal` interface is used in managed switch mode by default, but you can also use the interface in standalone mode. However, because the interface is accessed through the switch ports, you must make sure that the switch ports that connect to the network—usually the uplink ports—accept the VLAN ID assigned to `internal`, which is VLAN 4094, by default. For example, if you connect port24 to your upstream network infrastructure device, then you can assign VLAN 4094 as the native VLAN for port24 if you expect to receive untagged management traffic at that port. Alternatively, you can add VLAN 4094 to the allowed VLANs on port24 if you expect management traffic to be tagged.

The example on this slide shows how to set an IP address and the allowed administrative protocols on `internal`. Note that by default, `internal` doesn't allow any protocols. The example also shows how to change the VLAN ID on the uplink port (`port24` in the example). When you configure the allowed VLANs setting on a port, remember to also include other VLAN IDs for which you expect to receive tagged traffic from on the port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you set up basic management access on FortiSwitch, you can access its GUI for further configuration. The FortiSwitch GUI displays a left menu that is divided into the following four main sections:

- **System**: This section provides you with access to settings for switch management features, such as the internal and management interface, authentication servers, certificates, flow sampling, administrators, FortiSwitchCloud, as well as firmware and configuration maintenance. Moreover, when you log in to the FortiSwitch GUI, you land on the dashboard page of this section.

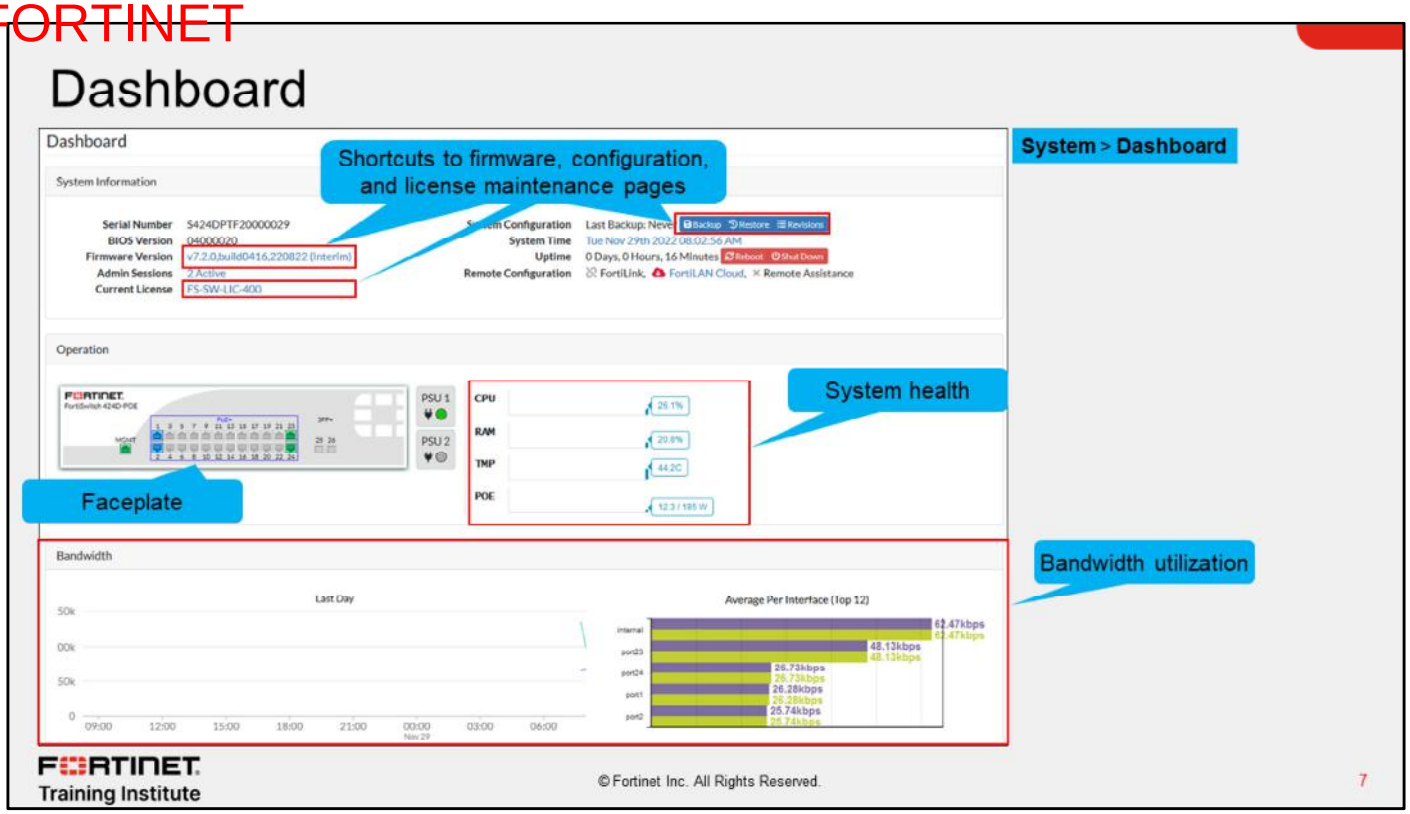
- **Switch**: Usually, this section is where you will spend most of your FortiSwitch management time. This is where you configure all switching-related aspects such as switch ports, VLANs, STP, ACLs, QoS, PoE, and so on.

- **Router**: This is where you configure static and dynamic routing. Dynamic routing options are displayed only if the switch has a valid advanced features license.

- **Log**: Browse this section to review system logs, as well as to configure logging on the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

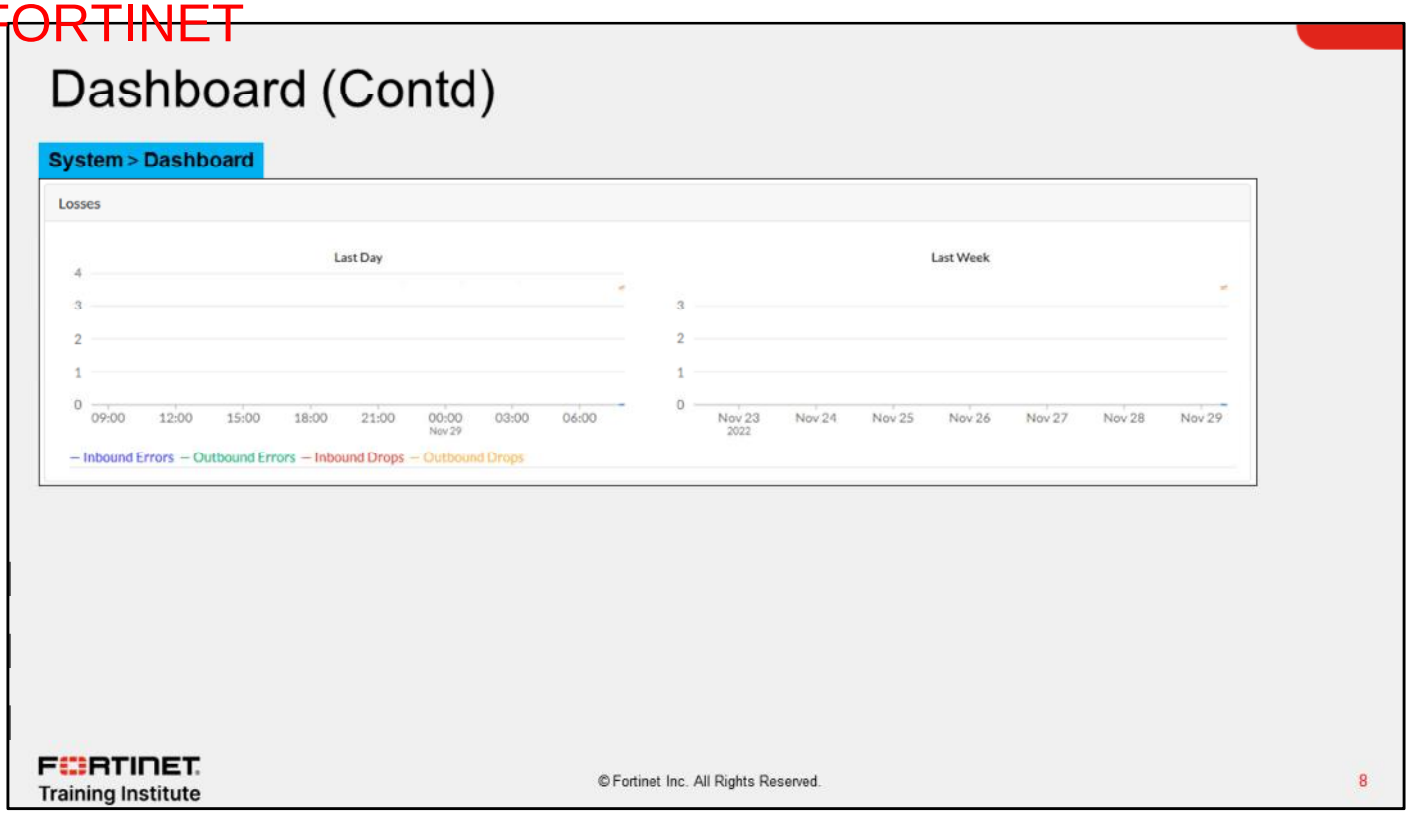


When you access the FortiSwitch GUI, you land on the **Dashboard** page. The page provides you with overall system management and operating information, and is organized in four sections:

- **System Information**: contains basic system information, such as the switch serial number, firmware version, time, and uptime. There are also links that provide you with quick access to the firmware, configuration, and license maintenance pages. You will also find links to reboot or shut down the switch.
- **Operation**: provides you with the faceplate view of the switch, which displays the status of ports. It also shows important health information, such as the current CPU and memory usage, the device temperature in Celsius degrees, and its PoE power consumption.
- **Bandwidth**: contains real-time graphs displaying the overall bandwidth utilization, as well as the top 12 bandwidth-consuming interfaces.
- **Losses**: contains real-time graphs displaying the packet loss on the switch due to port errors and drops. A screenshot of this section is shown on the next slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

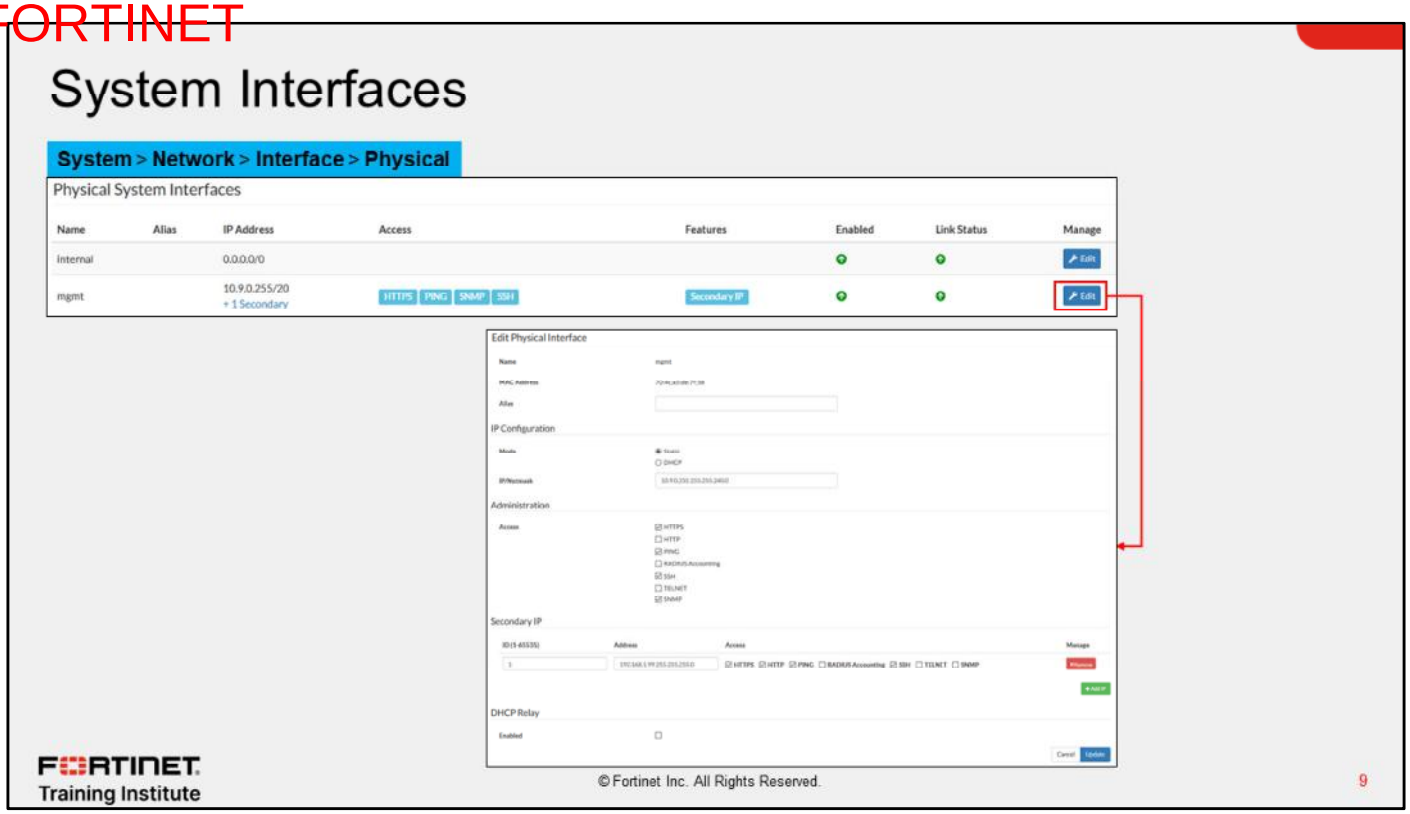


This slide shows a screenshot of the **Losses** section available on the dashboard. The graphs shown on this slide indicate no packet loss.

Next, you will learn about some of the most relevant GUI pages that administrators access to manage a standalone switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

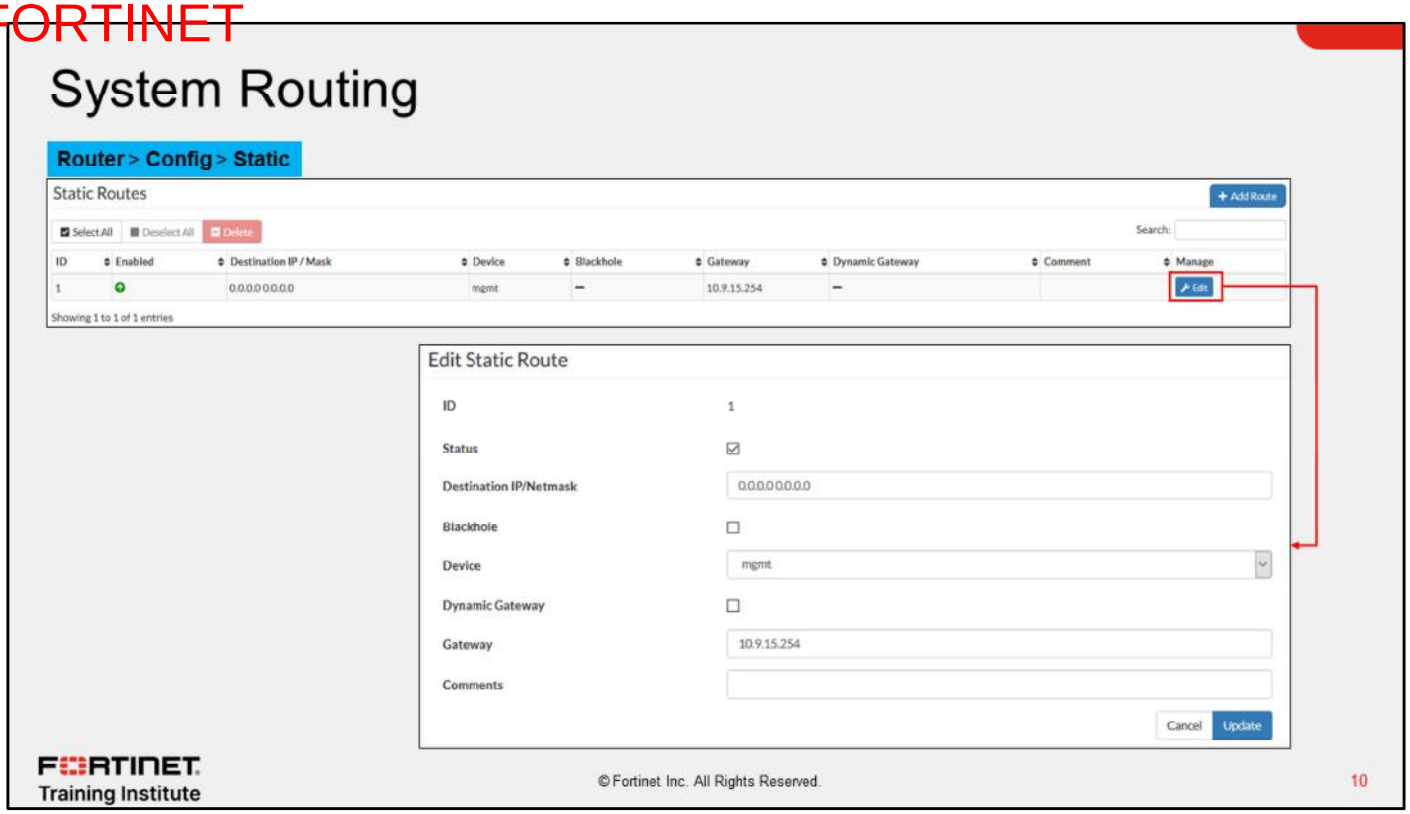
DO NOT REPRINT Brave-dumps.com
© FORTINET



If you need to make further changes to the system interfaces, you can do that by browsing to the **Physical System Interfaces** page, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

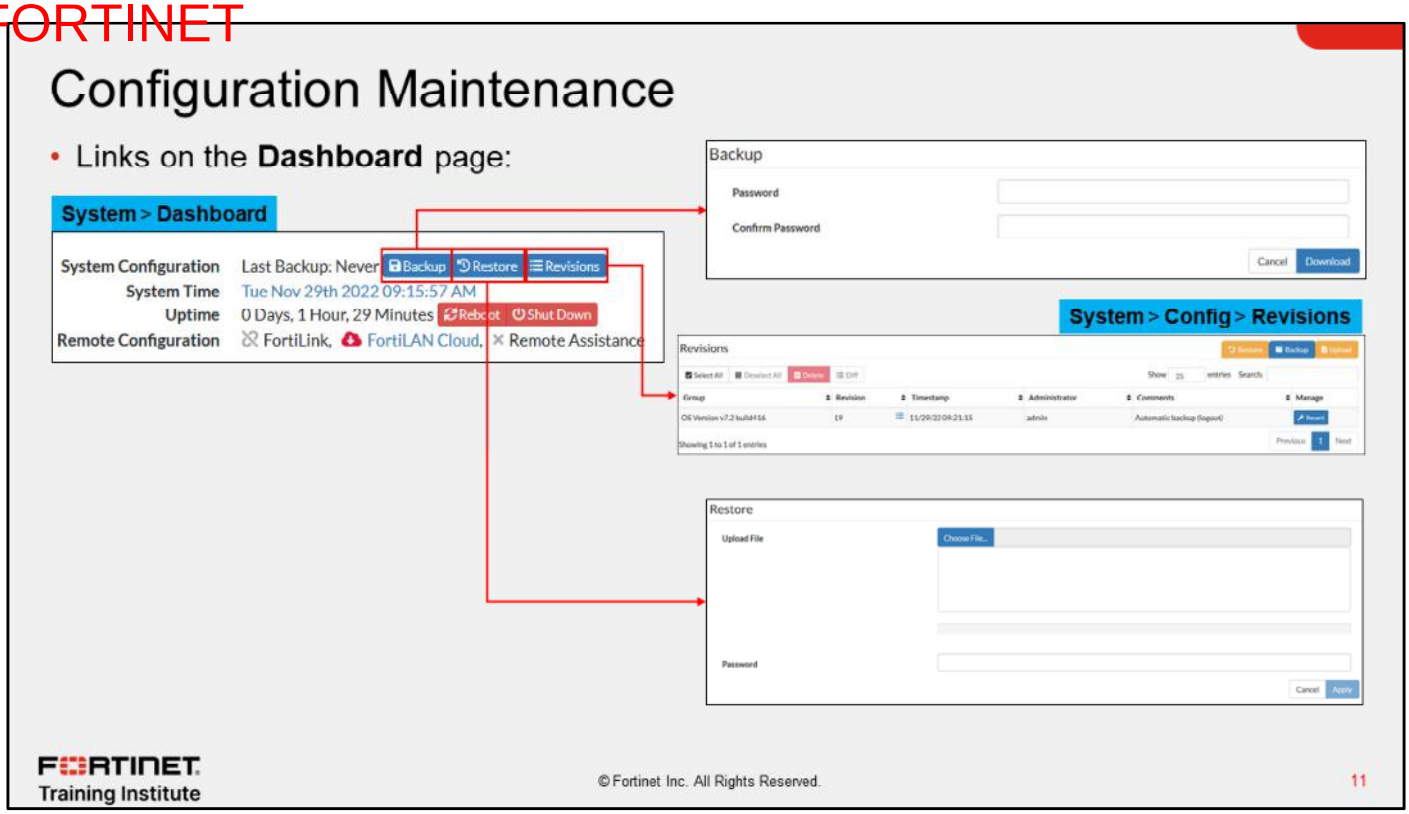
DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you want to access the switch from a different subnet, you likely need to configure one or more static routes for management traffic on the **Static Routes** page. This slide shows an example of a default route using the `mgmt` interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



For backing up and restoring the configuration, you must use the corresponding links available on the dashboard. For revisions, however, you can either use the link on the dashboard or just browse to the **Revisions** page under **System** > **Config**.

On the **Dashboard**, click **Backup** to download a copy of the switch configuration file. You can optionally set a password to encrypt the file for security purposes. After encryption, the configuration file cannot be decrypted without the password and a FortiSwitch device of the same model and firmware. If you don't set a password, most of the configuration file content is saved in plain text. However, sensitive information in the configuration file is hashed, and, therefore, obfuscated. The hashed sensitive information would include passwords for administrators, local users, and certificates. It may also include passwords for RADIUS and LDAP servers.

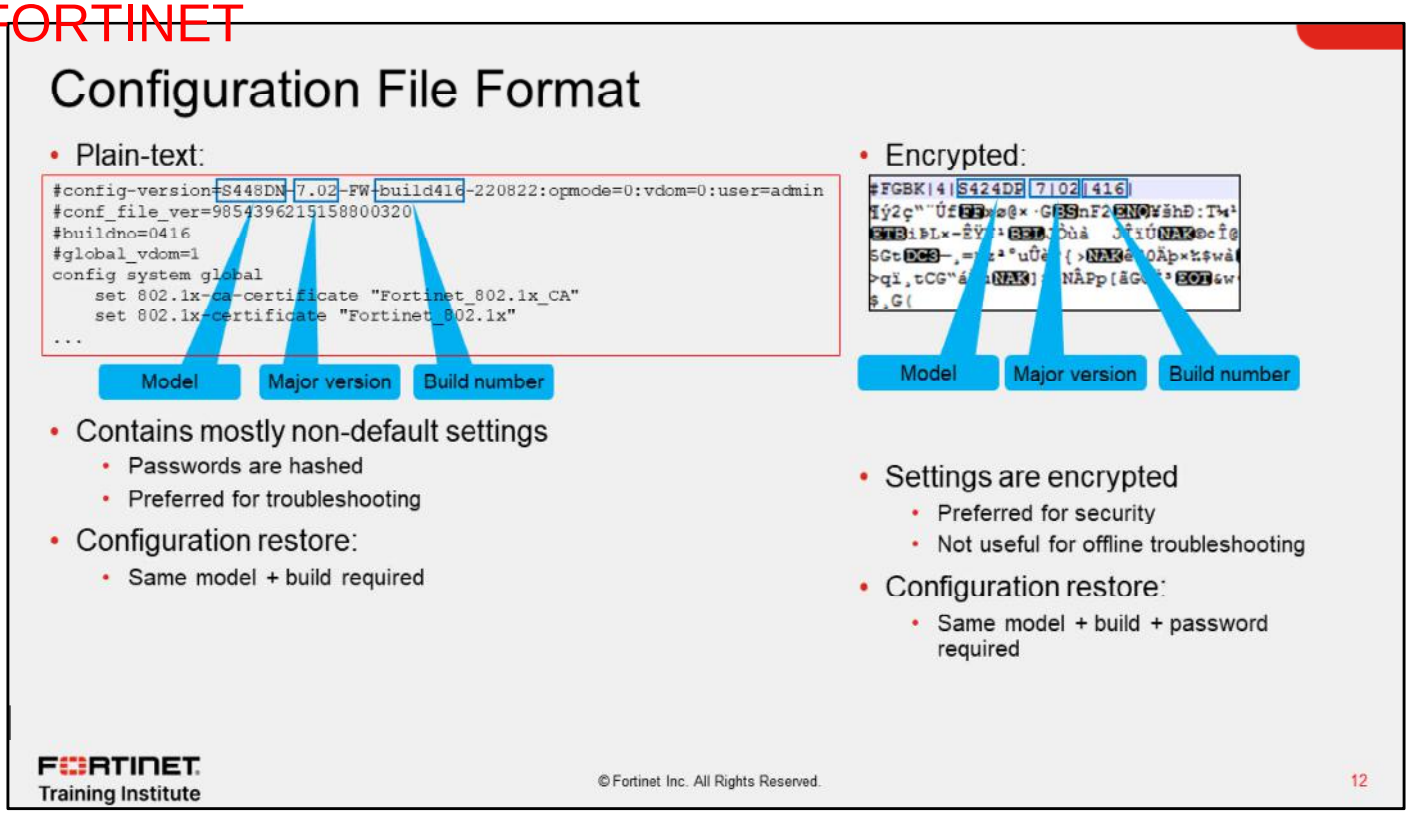
You have two options for restoring a configuration file: upload your own file or revert to any of the files automatically saved by FortiSwitch. Click **Restore** on the **Dashboard** to upload your configuration file. If the file is password-protected, make sure to enter its password so FortiSwitch can restore it.

The **Revisions** page displays a list of configuration files that have been automatically saved locally by the system. By default, this happens every time there is a change in the configuration and the administrator logs off from FortiSwitch either manually or automatically. The administrator logs off automatically when the administrative session times out, during a firmware upgrade, or when the device reboots. You can revert to any of the configuration files displayed on this page.

Note that restoring or reverting a configuration causes the switch to reboot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

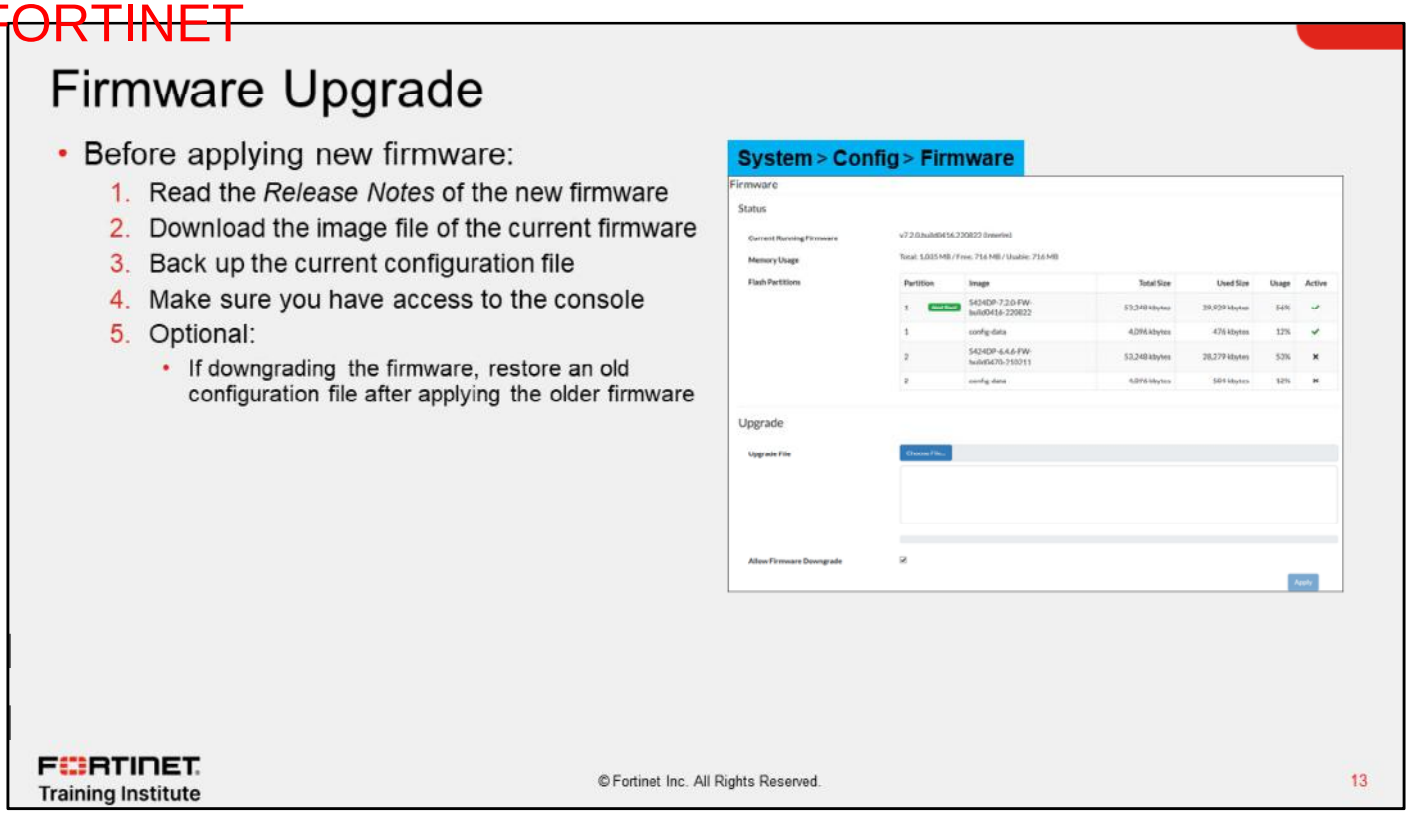


If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a plain text header that contains some basic information about the device. The example on this slide shows which information is included. To restore an encrypted configuration file, you must upload it to a FortiSwitch device of the same model and firmware, and then provide the password. To restore an unencrypted configuration file, you are required to match only the model and the firmware build number.

The configuration file contains mostly non-default settings. If the file is in plain text, passwords are hashed for privacy purposes. A plain text file is preferred for troubleshooting because you can review the configuration of the device offline, which is very useful and time saving when contacting Fortinet Technical Support. When the file is encrypted, you must check the configuration directly on the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



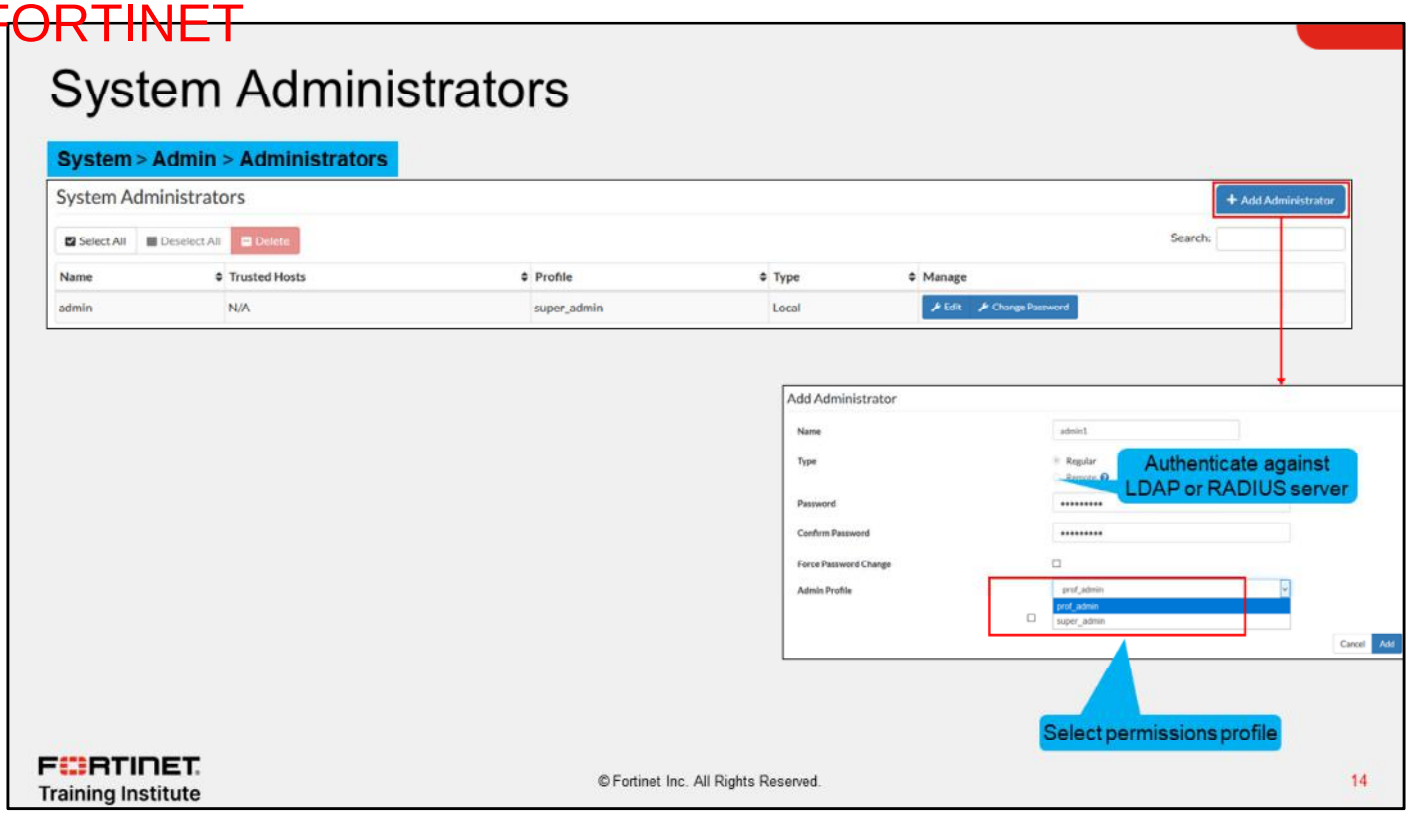
The example on this slide shows a screenshot of the **Firmware** page. Before applying new firmware to FortiSwitch, make sure to follow the following recommendations:

1. Read the *Release Notes* of the new firmware. The document contains important information about the recommended upgrade path. It also includes information about known issues introduced in the new firmware and their solutions, if applicable.
2. Download the image file of the current firmware. You do this in case you want to revert to the old firmware should you run into issues with the new firmware.
3. Back up the current configuration file. Having a backup is useful for troubleshooting or for reverting to an old configuration during a rollback.
4. Make sure you have access to the console. This enables you to monitor the firmware upgrade process, as well as capture any relevant messages produced on the console. The console is also useful if you happen to lose network connectivity to FortiSwitch after the upgrade.
5. Optionally, restore an old configuration file after downgrading the firmware. When you downgrade the firmware, some settings may be lost if the new firmware file doesn't understand the current configuration and, therefore, is unable to apply it. It you took a backup of the configuration file when FortiSwitch was running the older firmware, then you should restore the old configuration to ensure no settings are lost.

Upgrading the firmware is straightforward: Select an image file from your local workstation, and then click **Apply**. Make sure to select **Allow Firmware Downgrade** if the firmware image version you uploaded is older than the current version FortiSwitch is running. Note that upgrading or downgrading the firmware requires a reboot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

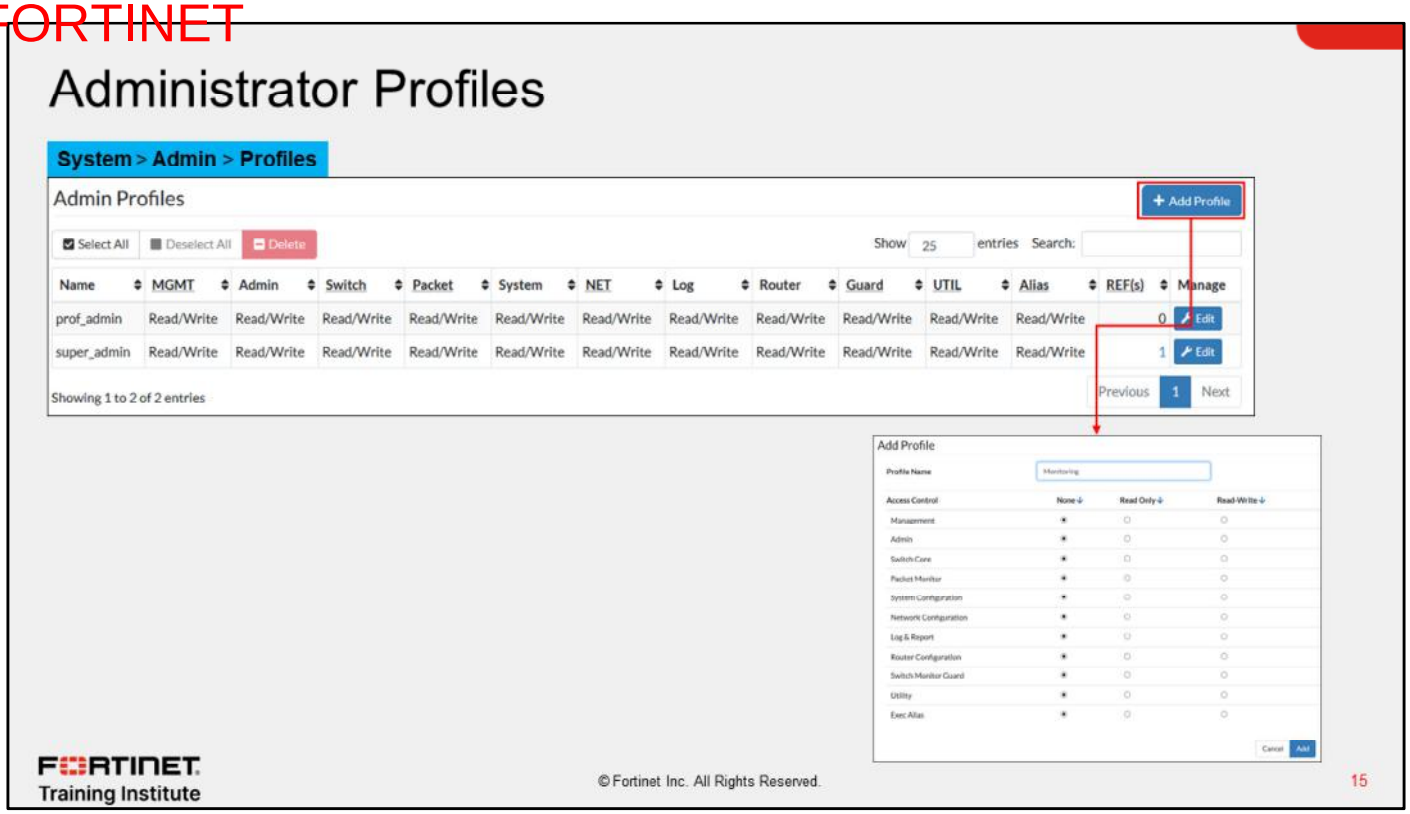


You can create a new system administrator or edit an existing one on the **Administrators** page. When editing an administrator, you can set its type to **Regular** or **Remote**. The former uses a local password for authentication, while the latter uses a password stored in a remote LDAP or RADIUS server.

Usually, you also want to limit the administrator permissions by assigning an **Admin Profile**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



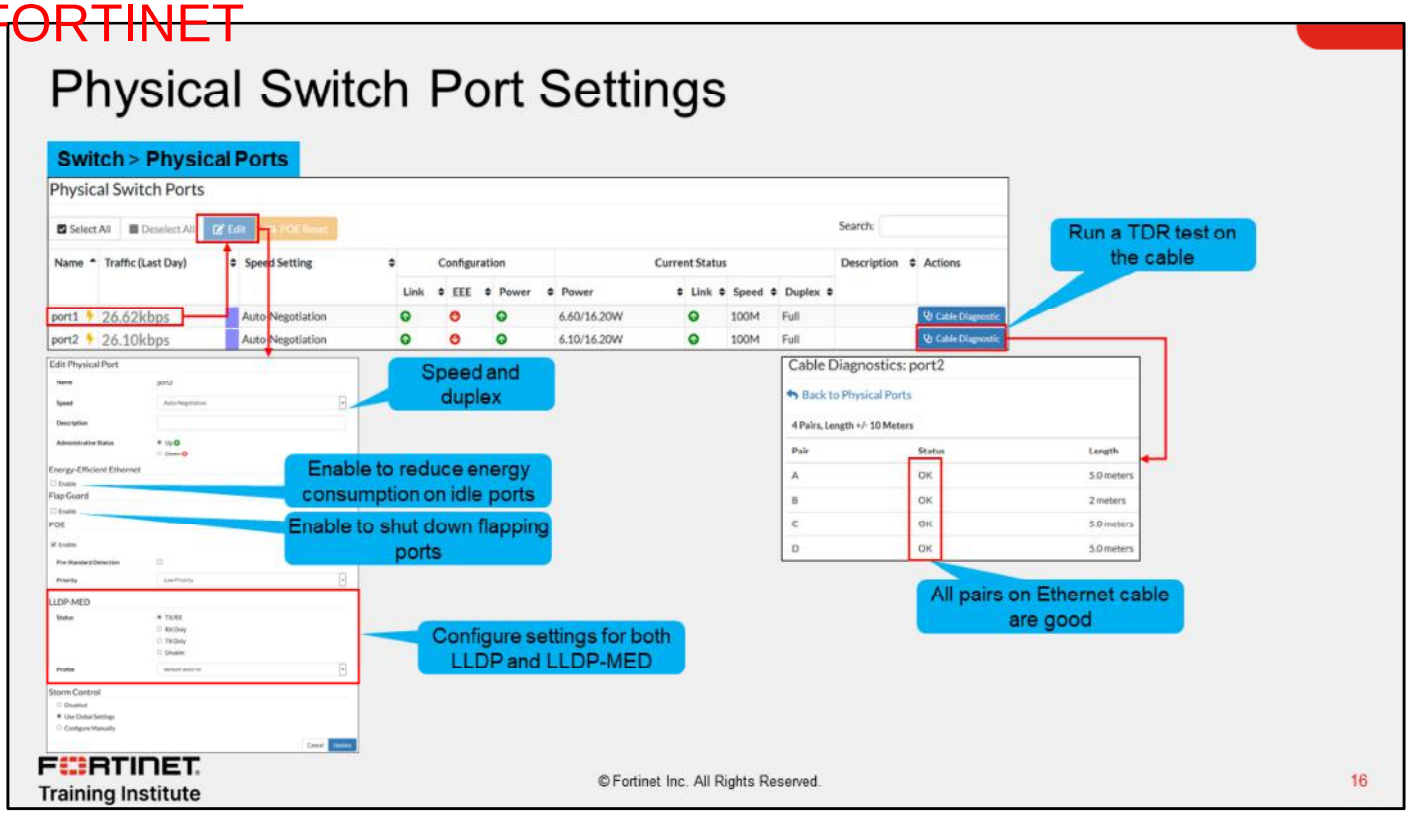
You assign permissions to an administrator profile on the **Admin Profiles** page. Here, you can specify read and write rights, read-only rights, or none. In addition, you assign the rights to a specific system configuration scope (or access control).

By default, there is a special profile named **super_admin**, which is used by the default account **admin**. It cannot be changed, and it provides full access to everything, making the admin account similar to a root superuser account.

The **prof_admin** is another default profile. It also provides full access, but unlike **super_admin**, which can create other **super_admin** users, administrators who are assigned the **prof_admin** profile can't. Also, you can change the permissions of the **prof_admin** profile, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The configuration for ports and trunks are organized in physical and interface settings. Physical settings, which are shown on the **Physical Switch Ports** page, are mostly settings for specific Layer 1 and Layer 2 features. For instance, you can set the port speed and duplex mode, shut down or bring up the port administratively, configure the port LLDP settings, and so on.

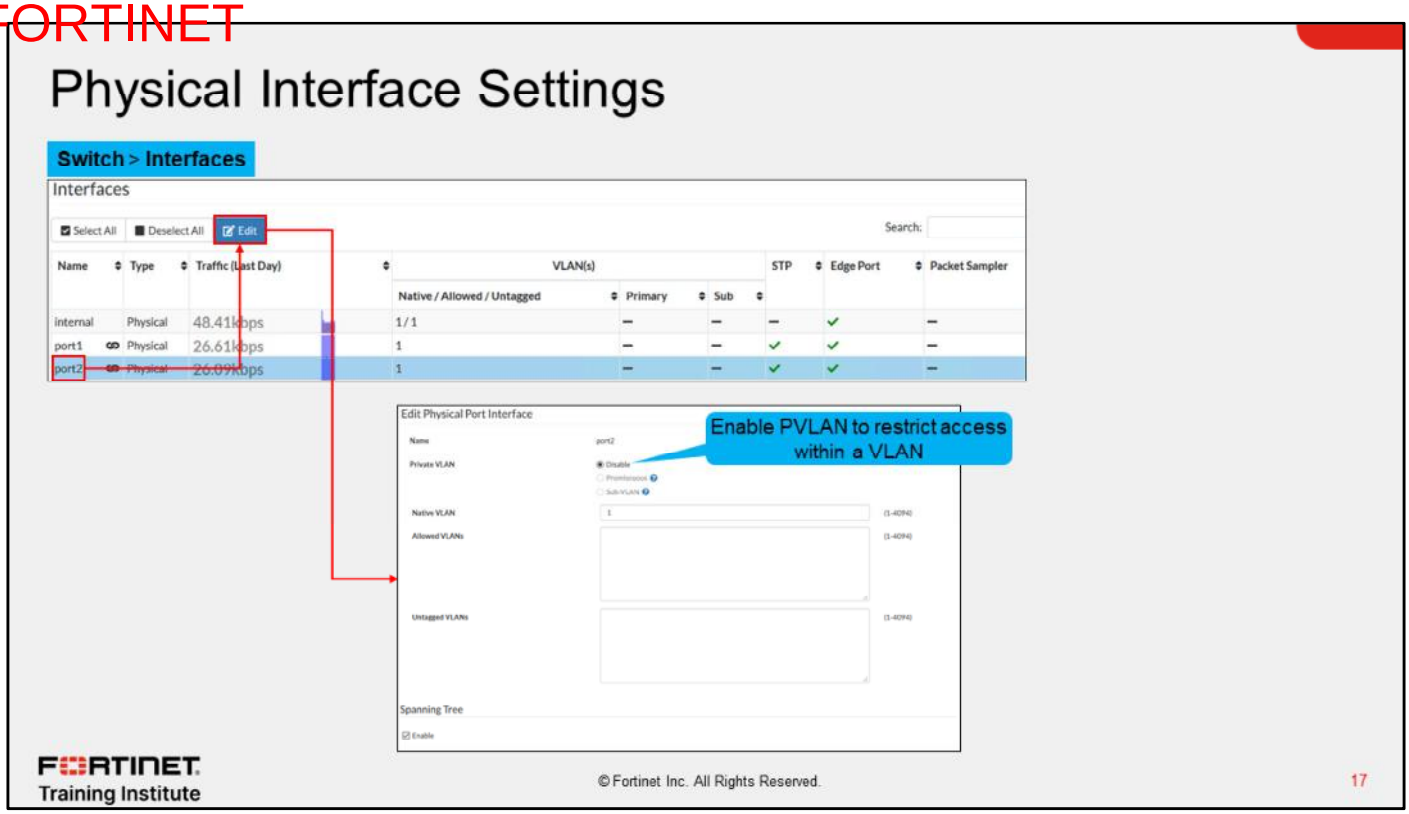
Another two options available on this page are energy-efficient Ethernet (EEE) and flap guard. When you enable EEE, the switch monitors the traffic on a port and places the port in sleep mode if no data is being transmitted. When data transmission is resumed, the port starts consuming the normal amount of power again.

Flap guard prevents STP instability by detecting and automatically shutting down flapping ports. Because a port transitions through different STP states every time its link comes up, shutting down flapping ports can prevent the STP process from becoming unstable.

The **Physical Switch Ports** page also provides an option to run a time-domain reflectometer (TDR) diagnostic test on the cable. FortiSwitch uses TDR to determine an estimated length of each pair on the Ethernet copper cable, as well as to detect if a pair is faulty. The example on this slide shows good TDR test results for all pairs in the Ethernet cable connected to port2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



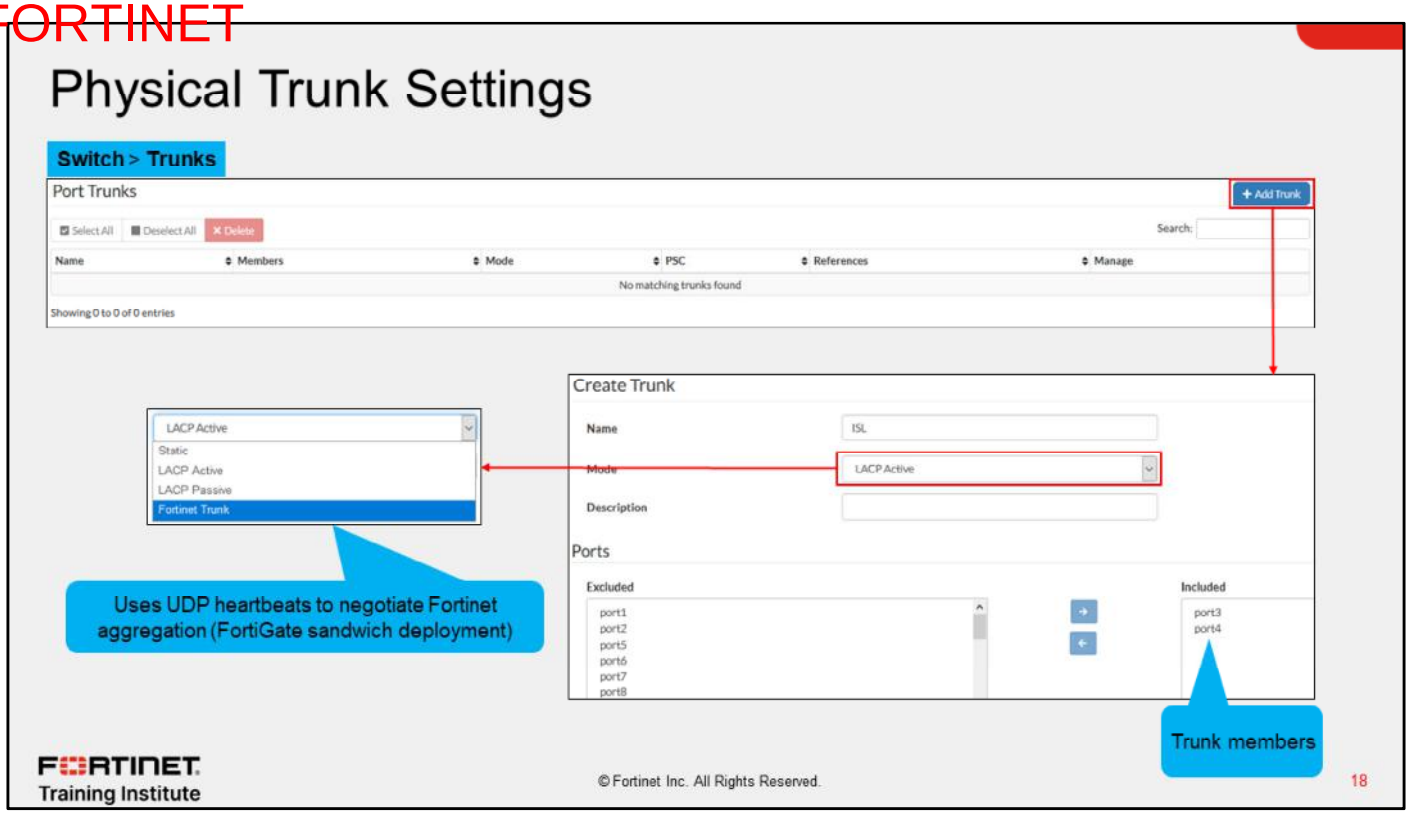
Most of the switch port settings are found on the **Switch Interfaces** page. This is where you configure the port VLAN settings, STP, QoS, IGMP snooping, packet and flow sampling, port security, and so on.

A feature that is more suited for standalone deployments is **Private VLAN** (PVLAN). PVLAN divides a primary VLAN into one or more secondary VLANs. The goal is to further restrict access of endpoints in a VLAN without having to change their current IP addressing. You will learn more about PVLANs in this lesson.

The example on this slide shows some of the settings available on the **Switch Interfaces** page when you edit a port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



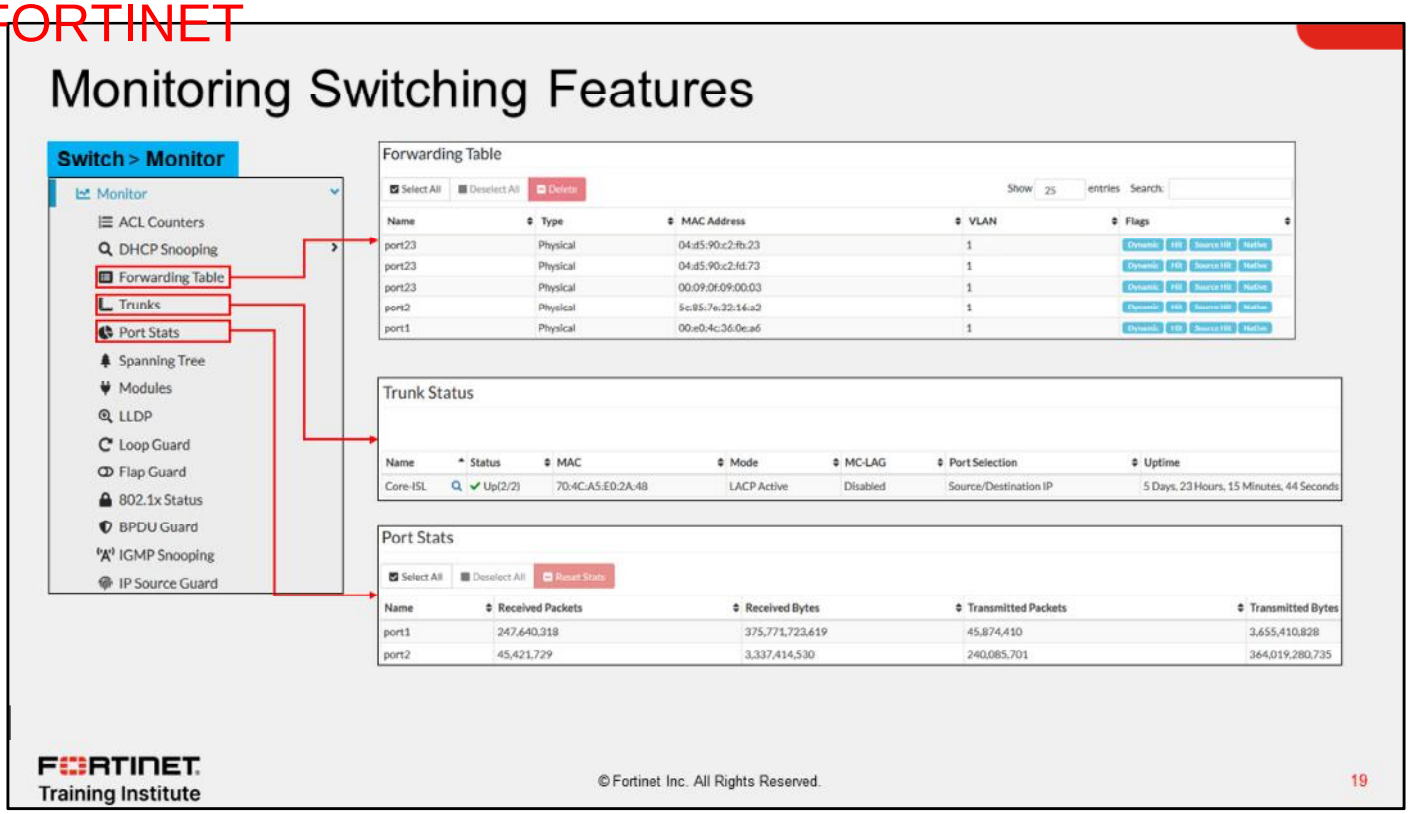
You can also create trunks by browsing to the **Trunks** page. When editing or creating a trunk, you can select a trunk mode that is only available in standalone mode: **Fortinet Trunk**.

The Fortinet trunk mode was created with a specific topology in mind: *FortiGate sandwich deployment*. Under this scenario, you have one or more FortiSwitch devices receiving traffic from the network and forwarding it to one or more sandwiched FortiGate devices for inspection. After FortiGate inspects and accepts the traffic, the traffic is forwarded back to FortiSwitch. It is called a sandwich because FortiSwitch load balances the traffic across multiple FortiGate devices. To load balance the traffic, you configure one or more trunks on FortiSwitch, with each trunk member connected to a different FortiGate.

Unlike LACP, which uses LACPDUs to monitor the health of trunk members, a Fortinet trunk uses UDP for heartbeat packets. This mechanism enables FortiSwitch to check the health of the connected sandwiched FortiGate devices by verifying that the heartbeat packets sent on a trunk member are received at the same member, preventing FortiSwitch from sending traffic to a dead FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

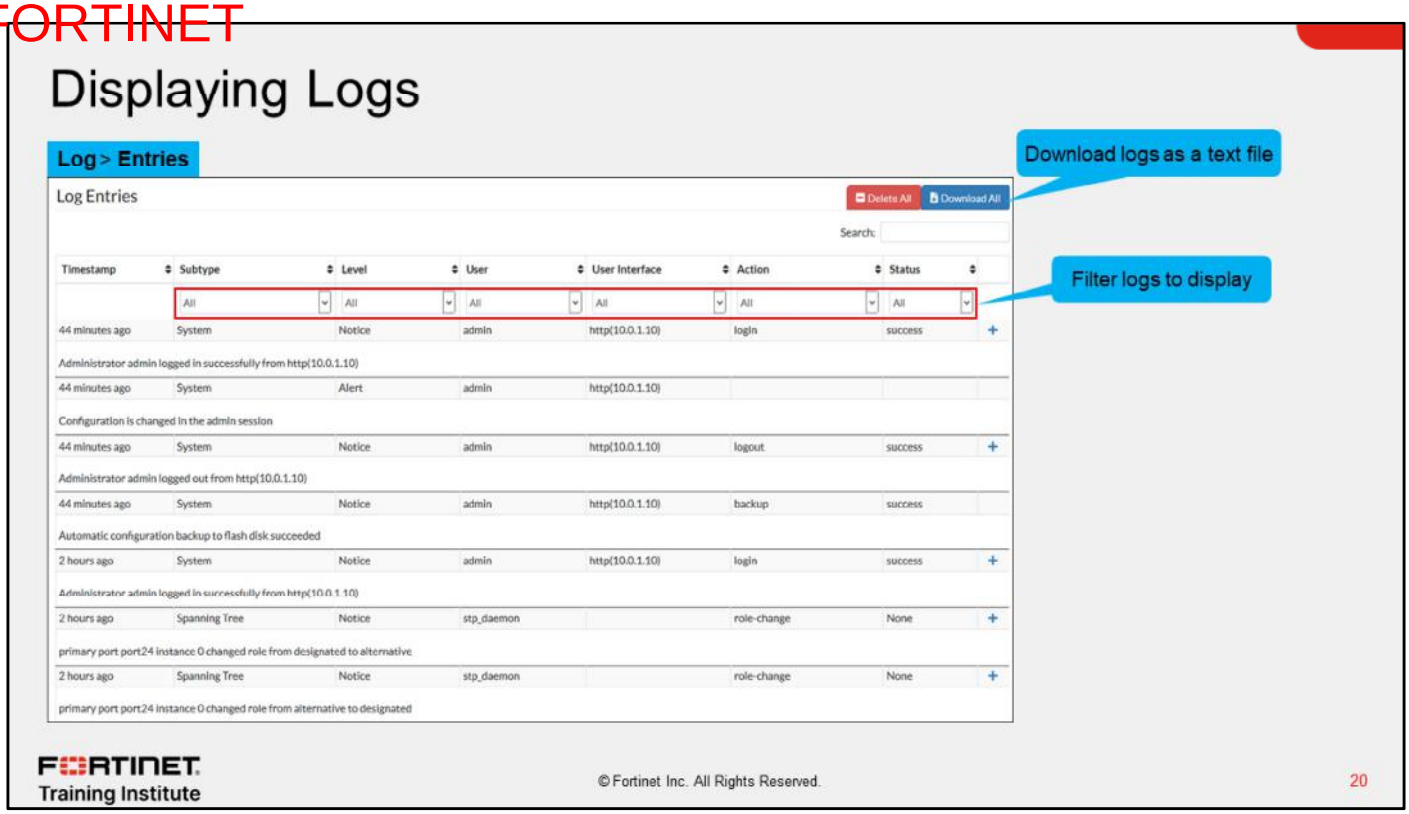
DO NOT REPRINT Brave-dumps.com
© FORTINET



Another important page that you will likely visit is the **Monitor** page located under the **Switch** menu. Here you find status information for multiple switching-related features, such as the MAC address table (or forwarding table), trunks, port stats, and STP. The example on this slide shows screenshots of the **Forwarding Table**, **Trunks**, and **Port Stats** pages.

Vouchers & Dumps are Available | WhatsApp +201224560923

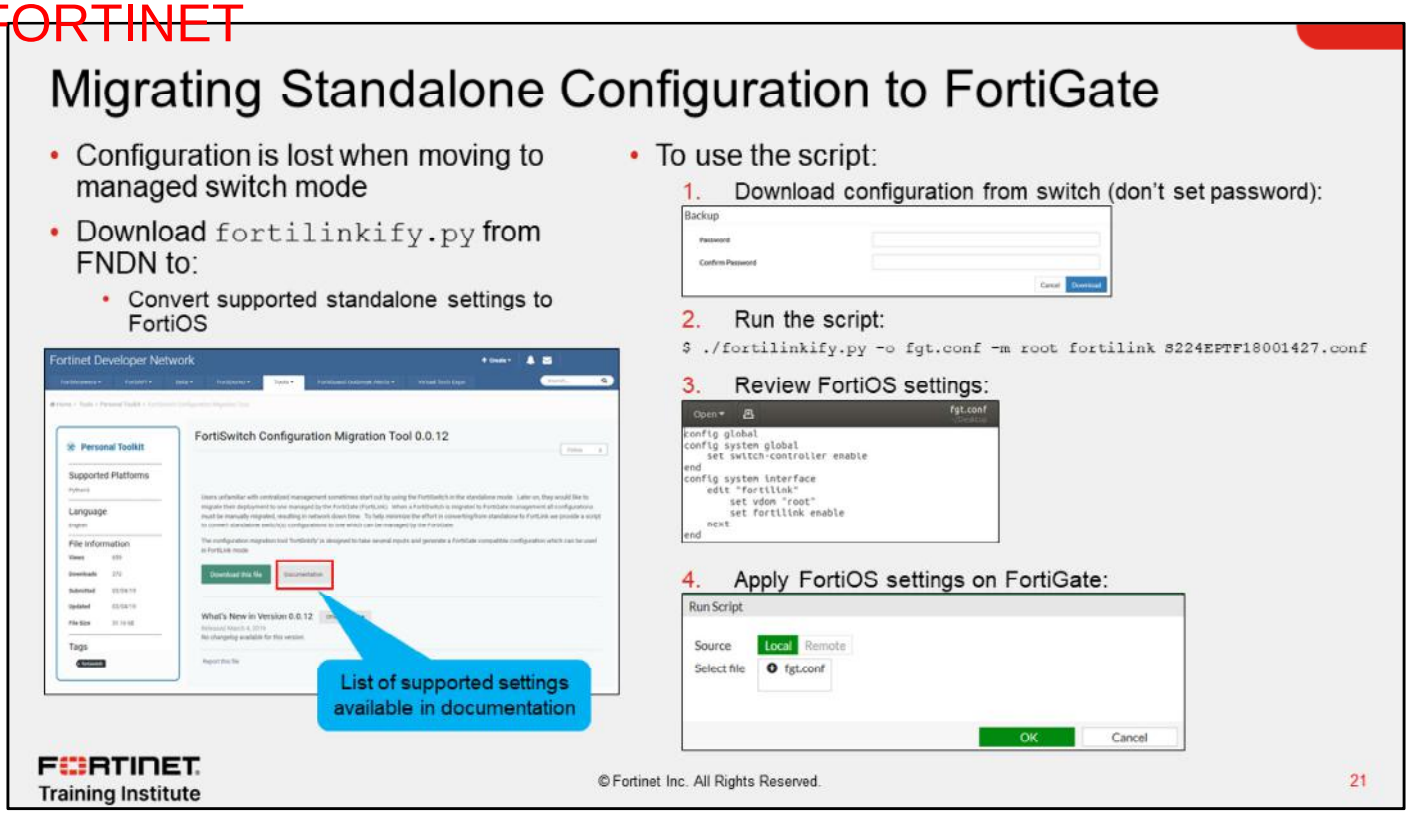
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Browse to the **Log** page to display the local logs generated by the system. Here, you can download the logs as a text file or delete them. There are also a filter tool bar and a search bar that you can use to display specific logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Most administrators deploy FortiSwitch in managed switch mode. However, some administrators who are unfamiliar with managed switch mode prefer to deploy FortiSwitch in standalone mode first, and then eventually move to a FortiGate-managed setup.

When you enable managed switch mode on FortiSwitch, the configuration on the standalone switch is replaced by the default configuration for a managed switch, which means that your standalone settings are lost. This also means that you must start your FortiSwitch configuration over again, but this time using FortiGate. To save time, Fortinet provides you with a migration tool called `fortilinkify.py` that is available for download on the Fortinet Developer Network (FNDN) page at `fndn.fortinet.net`.

The tool is a Python script that converts the supported settings in a FortiSwitch standalone configuration file to the equivalent FortiOS settings for a managed switch. Note that not all the settings in your FortiSwitch configuration file are converted. Only those supported by managed switch mode and by the script are. The tool documentation at the FNDN page contains a list of supported settings.

To use the script:

1. Download the configuration file from your standalone switch. Don't set a password.
2. Run the script. The script takes as input the configuration file from your standalone switch and generates a configuration file with the equivalent FortiOS settings.
3. Review the configuration file generated by the script. You should be aware of the changes that you will apply on FortiGate.
4. Apply the configuration file on FortiGate. For this, you can use the FortiGate GUI script tool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the factory default secondary IP address assigned to the mgmt interface?
   - ✓ A. `192.168.1.99 255.255.255.0`
   - B. `192.168.100.99 255.255.255.0`

2. Which statement about the factory default settings on the internal interface is true?
   - A. SSH, HTTP, and HTTPS access is enabled.
   - ✓ B. The native VLAN is set to 4094.

3. Which statement about migrating a standalone configuration to FortiGate is true?
   - ✓ A. You can use the `fortilinkify.py` tool available on FNDN to convert the switch configuration to FortiOS.
   - B. The standalone configuration is kept after the management mode is changed to managed switch mode.

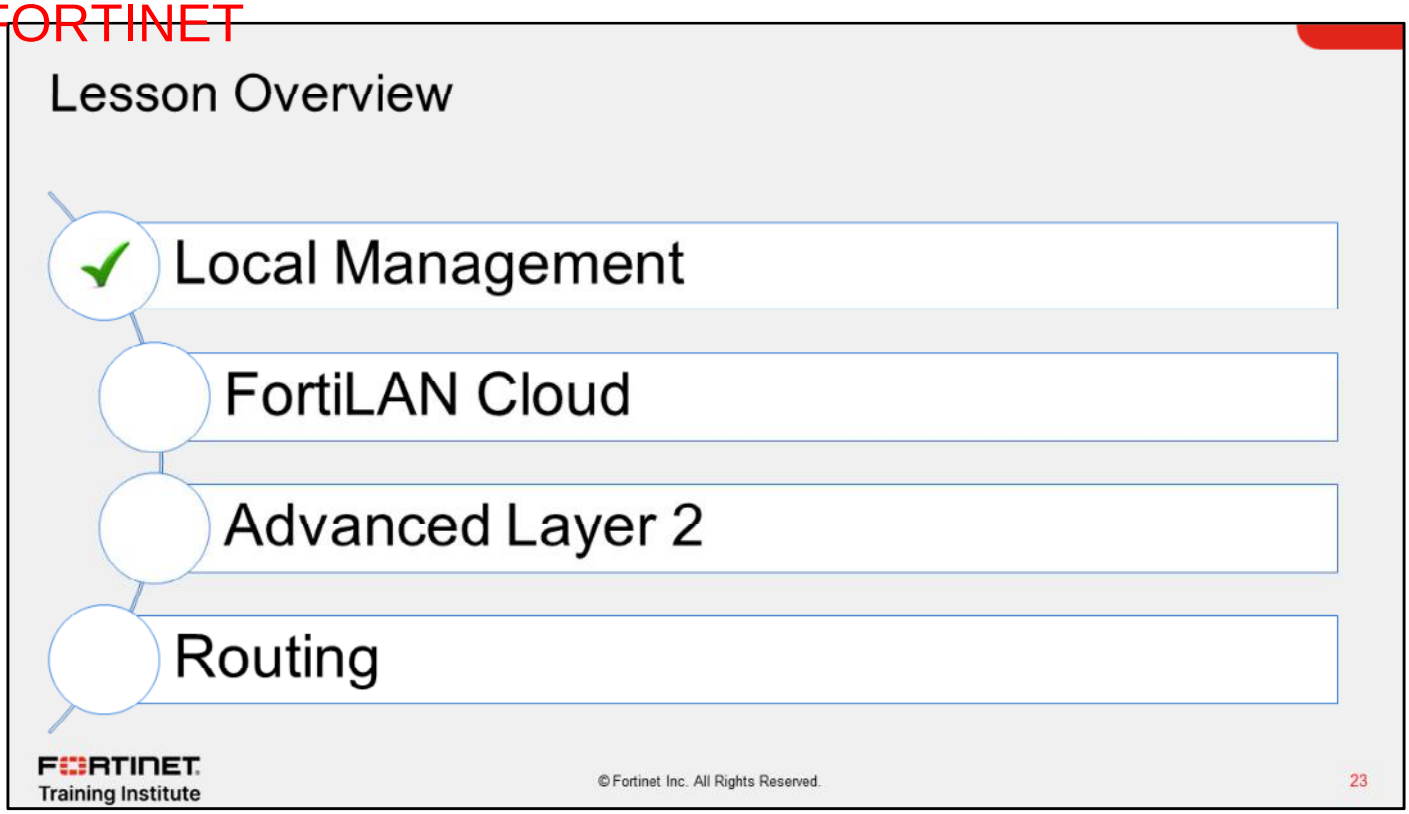
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

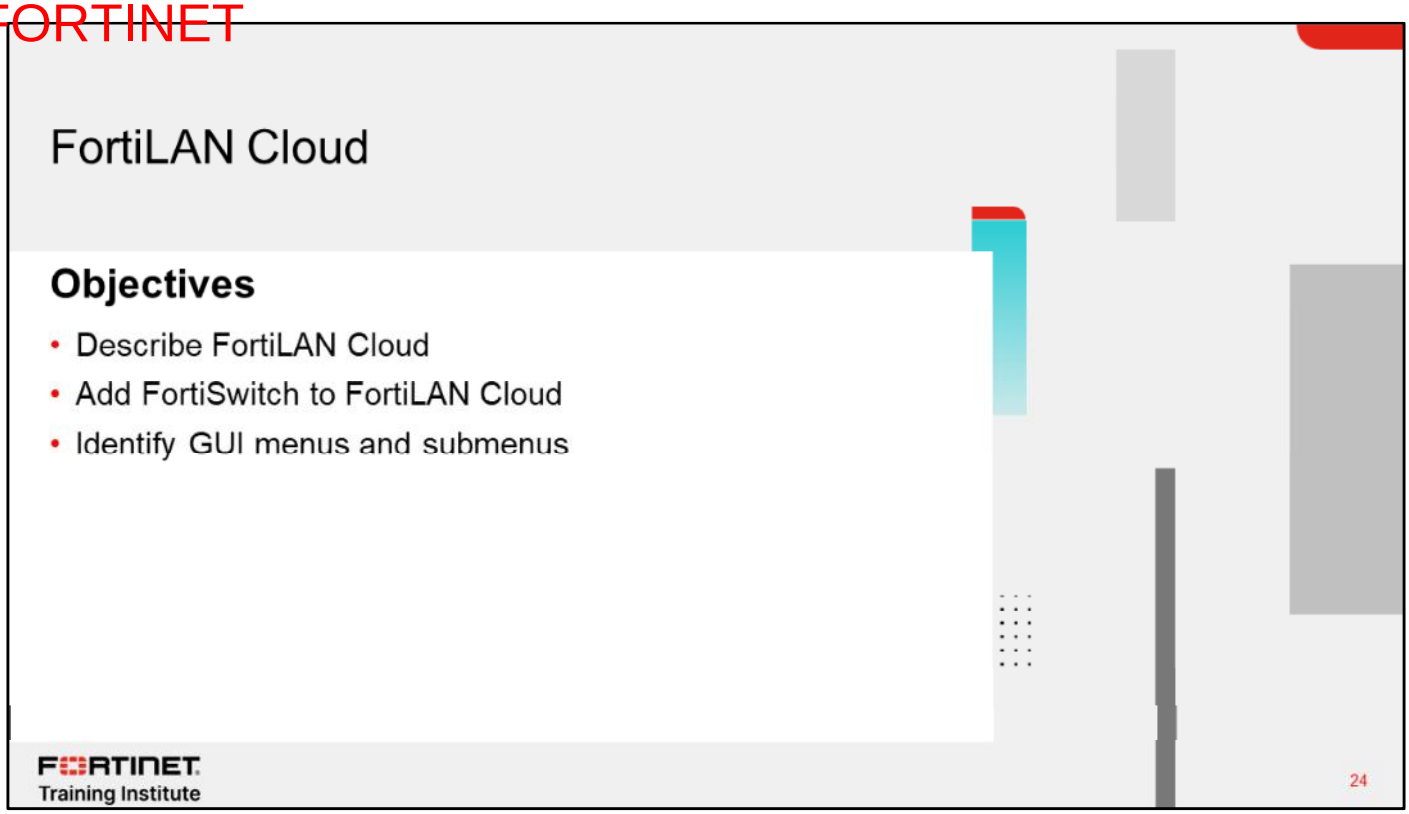


Good job! You now understand local management.

Now, you will learn about FortiLAN Cloud.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

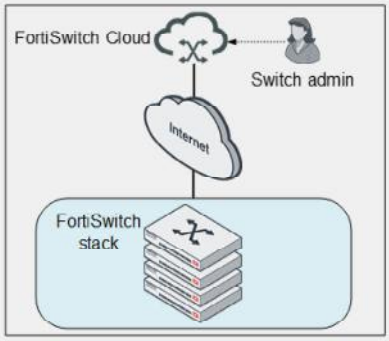
By demonstrating competence in FortiLAN Cloud, you should be able to understand how to manage one or more FortiSwitch islands from FortiLAN Cloud.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiLAN Cloud

- Cloud-based MaaS for standalone switch
  - `fortilan.forticloud.com`
- Log in using current Fortinet support account
- Requirements:
  - FortiSwitch:
    - Internet connection
    - Valid support contract
  - Fortinet support account:
    - Register FortiSwitch
    - Valid FortiLAN Cloud license if you want to manage more than three devices
- Operation:
  - FortiSwitch initiates HTTPS connection to `fortiswitch-dispatch.forticloud.com`
  - FortiLAN Cloud polls data every 5 minutes




```
config system flan-cloud
    set status enable
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

FortiLAN Cloud—`fortilan.forticloud.com`—is a management as a service (MaaS) solution that provides centralized discovery, visibility, and configuration for standalone FortiSwitch devices and Fortinet wireless FortiAP devices, however, this course covers only FortiSwitch.

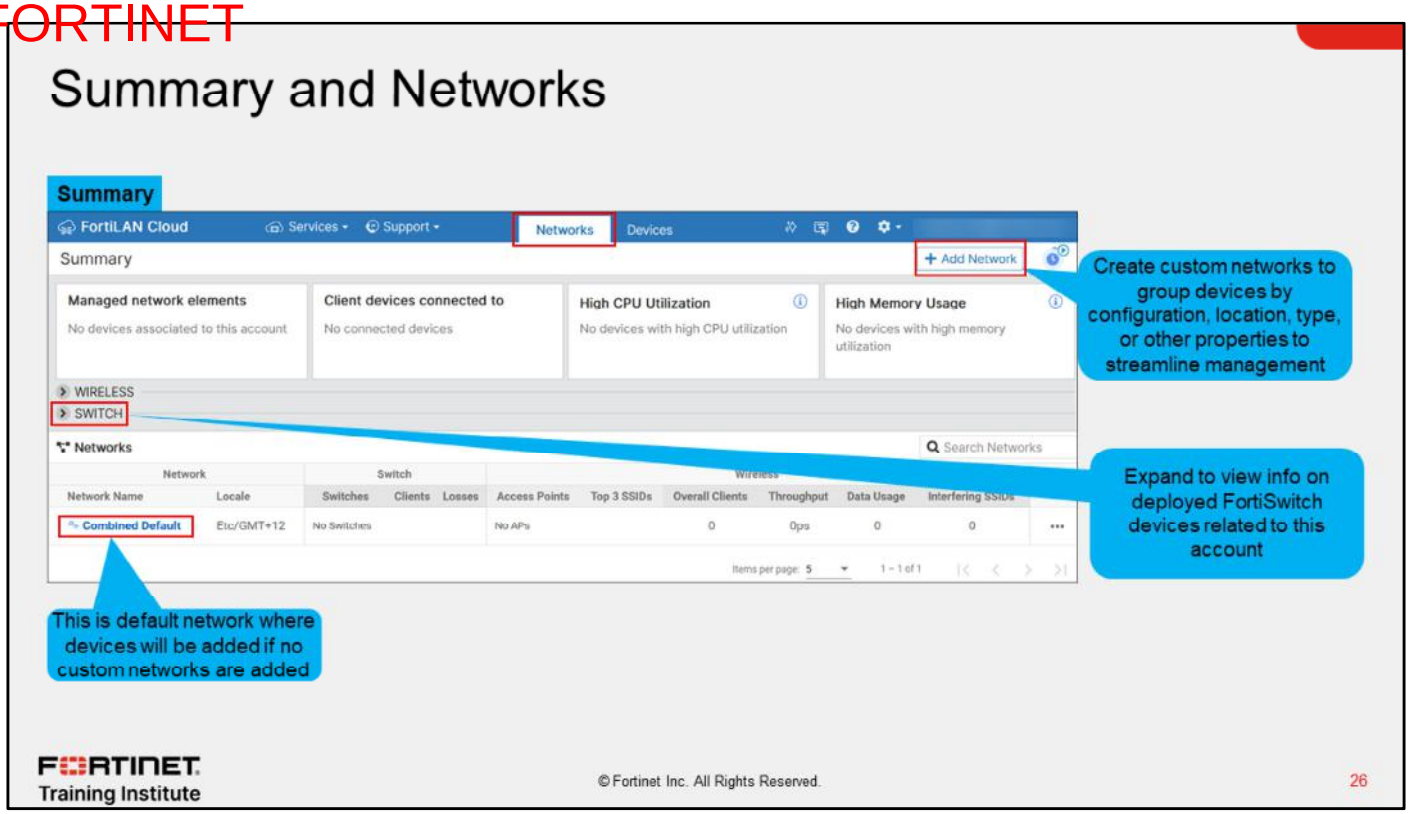
FortiLAN Cloud requires every switch to have internet access and a valid support contract. You must also register FortiSwitch on your Fortinet support account so you can add the device on FortiLAN Cloud. In addition, you must purchase a FortiLAN Cloud license if you want to manage more than three FortiSwitch devices.

FortiLAN Cloud is disabled by default. When enabled, FortiSwitch securely connects to `fortiswitch-dispatch.forticloud.com` on TCP port 443 using HTTPS. After the connection is established, FortiLAN Cloud polls data from FortiSwitch every 5 minutes.

This slide shows the FortiSwitchOS CLI setting that controls the FortiLAN Cloud feature on FortiSwitch. If you also want to manage your standalone switch from FortiLAN Cloud, ensure that the feature is enabled under `config system flan-cloud`.

Vouchers & Dumps are Available | WhatsApp +201224560923

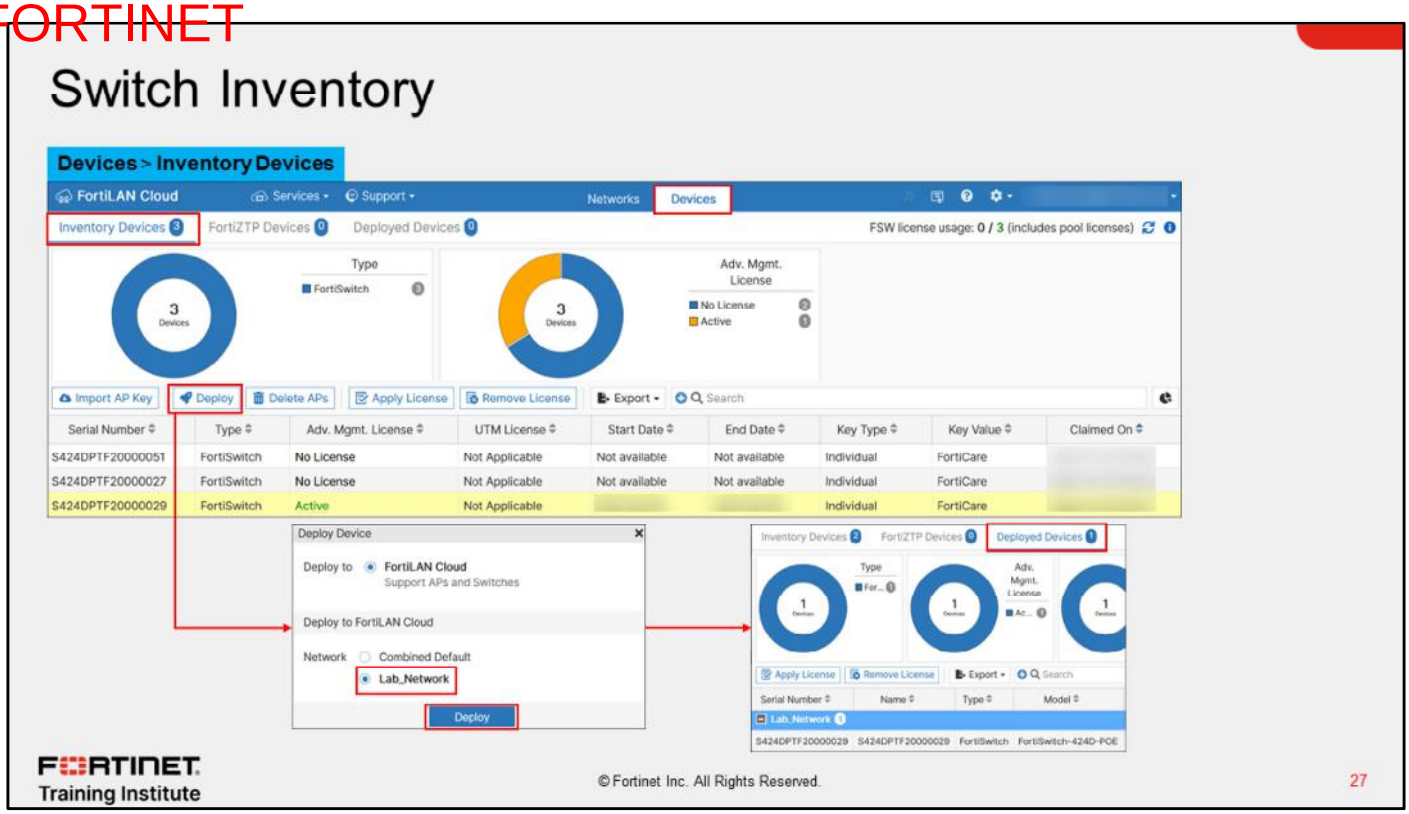
DO NOT REPRINT Brave-dumps.com
© FORTINET



After you log in to FortiLAN Cloud, you land on the **Networks** tab of the **Summary** page. From this page, you can access summary information of deployed FortiSwitch devices and events. FortiLAN Cloud uses networks to group devices together logically for management purposes. The default network is called *Combined Default* and all devices will be placed in this group if no custom groups are defined. You create custom networks from this page by clicking the **Add Network** button. To select the network containing the devices you want to manage, click the network name in the **Network** section at the bottom.

Vouchers & Dumps are Available | WhatsApp +201224560923

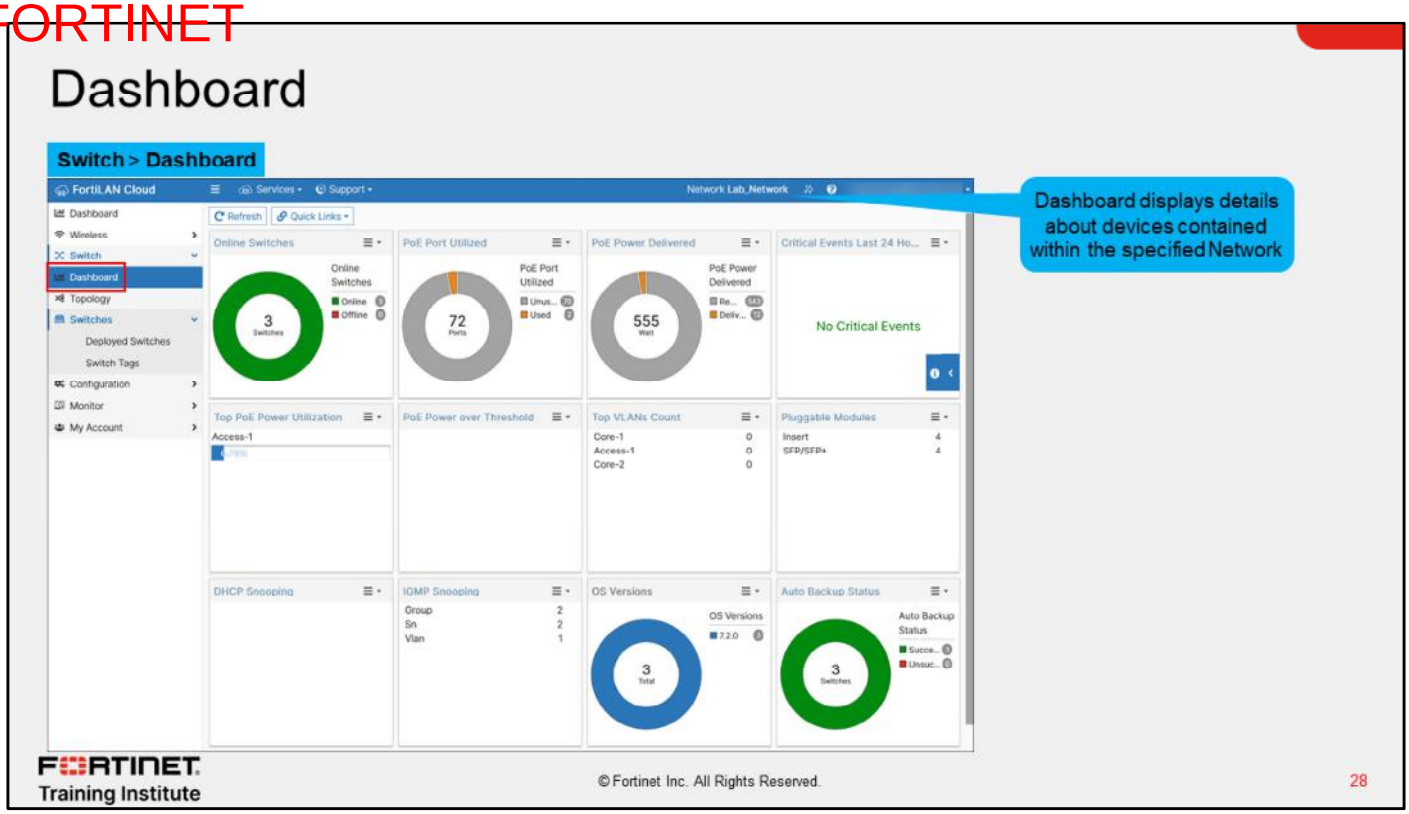
DO NOT REPRINT Brave-dumps.com
© FORTINET



Inventory Devices on the **Devices** tab displays FortiSwitch devices that are registered to the Fortinet account but not deployed to FortiLAN Cloud for management. From this page, you deploy one or more FortiSwitch devices to FortiLAN Cloud by selecting the devices and clicking **Deploy**. You assign the devices to their respective network so that they are grouped accordingly during the deployment process. After a FortiSwitch device is deployed, it is no longer displayed under **Inventory Devices**—it moves to **Deployed Devices**. In the example shown on this slide, a FortiSwitch is deployed to the network called **Lab_Network**, the **Inventory Devices** counter is reduced from 3 to 2, and the **Deployed Devices** counter is increased from 0 to 1 after this operation takes place.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

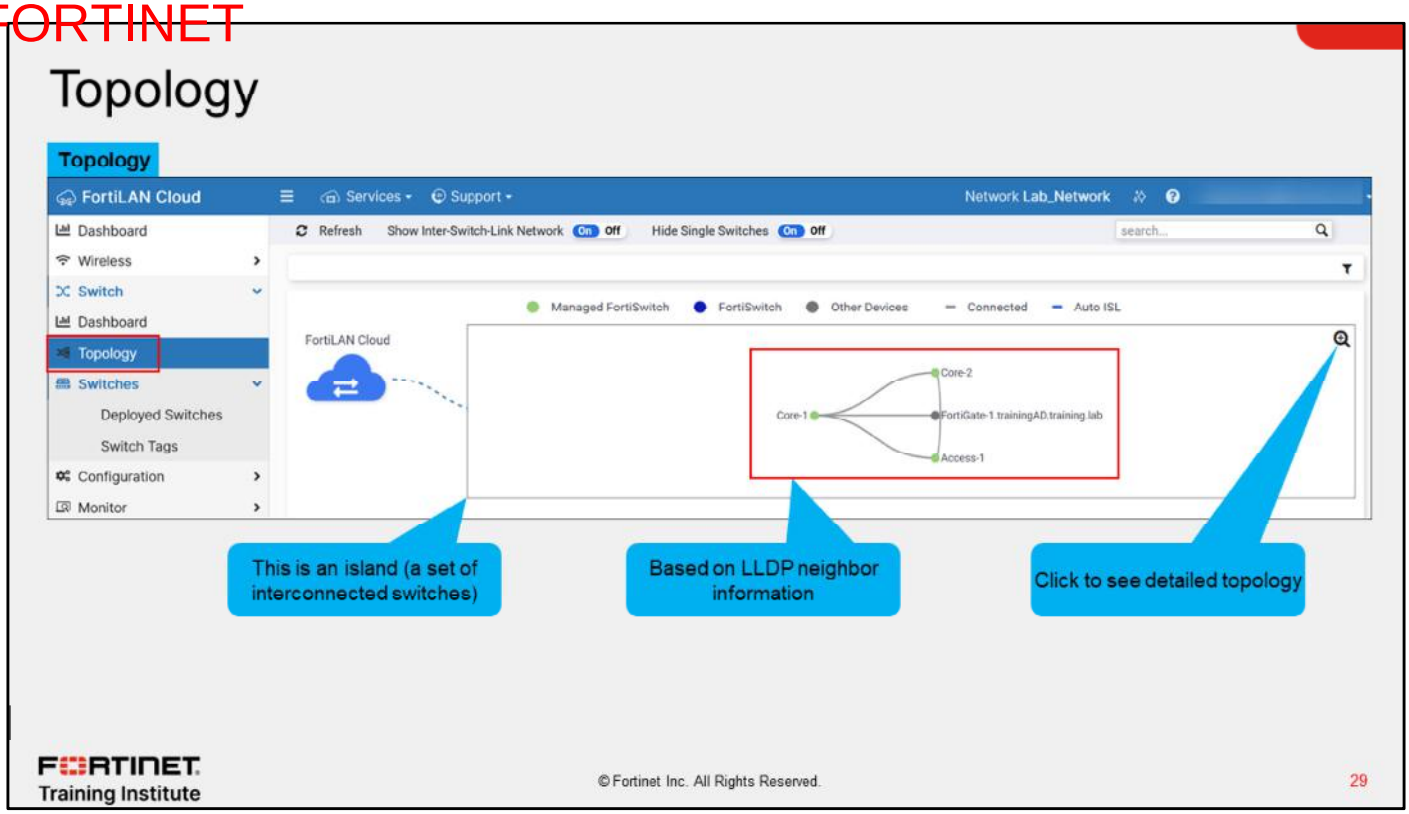


After you add one or more FortiSwitch devices, you can browse to the **Dashboard** page under the **Switch** menu, where you can get a status summary of your switches. There are multiple widgets on the page, each reporting on a different FortiSwitch feature. Each dashboard is relative to the Network object you've selected. In the example shown on this slide, the network named *Lab_Network* was selected and so only the FortiSwitch devices that were added to that network are displayed.

Each widget contains links that provide you with further details about the feature in question. Note that the sample screenshot was cropped to fit on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



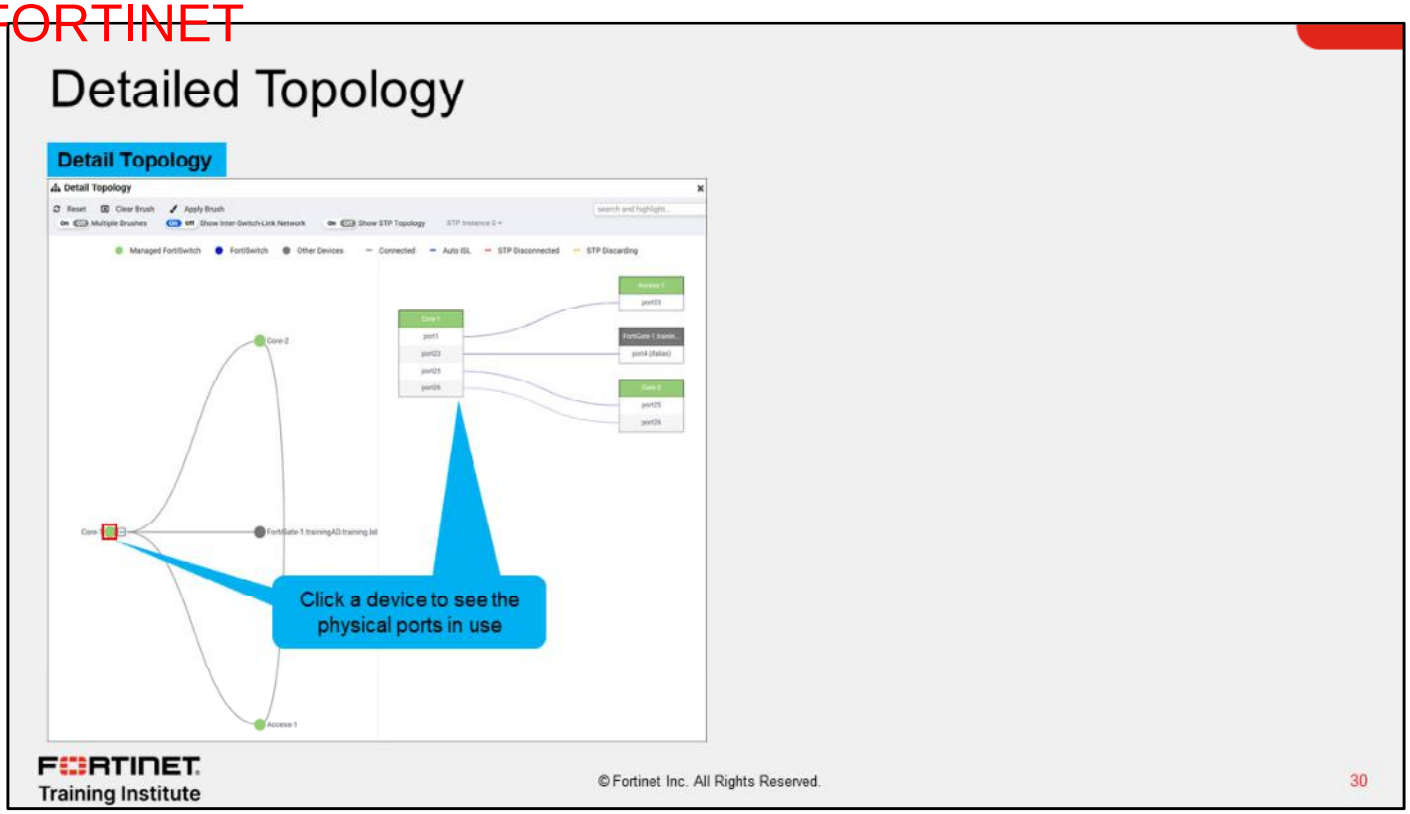
Click **Topology** to view a physical topology built based on the LLDP neighbor information discovered by your switches. The page displays a physical topology for each FortiSwitch island managed by FortiLAN Cloud. An island is a group of interconnected FortiSwitch devices. The example on this slide shows one FortiSwitch island only.

Only physical connections for which an LLDP neighbor has been discovered are included in the topology.

You can also click the zoom icon to display a detailed view of the physical connections.

Vouchers & Dumps are Available | WhatsApp +201224560923

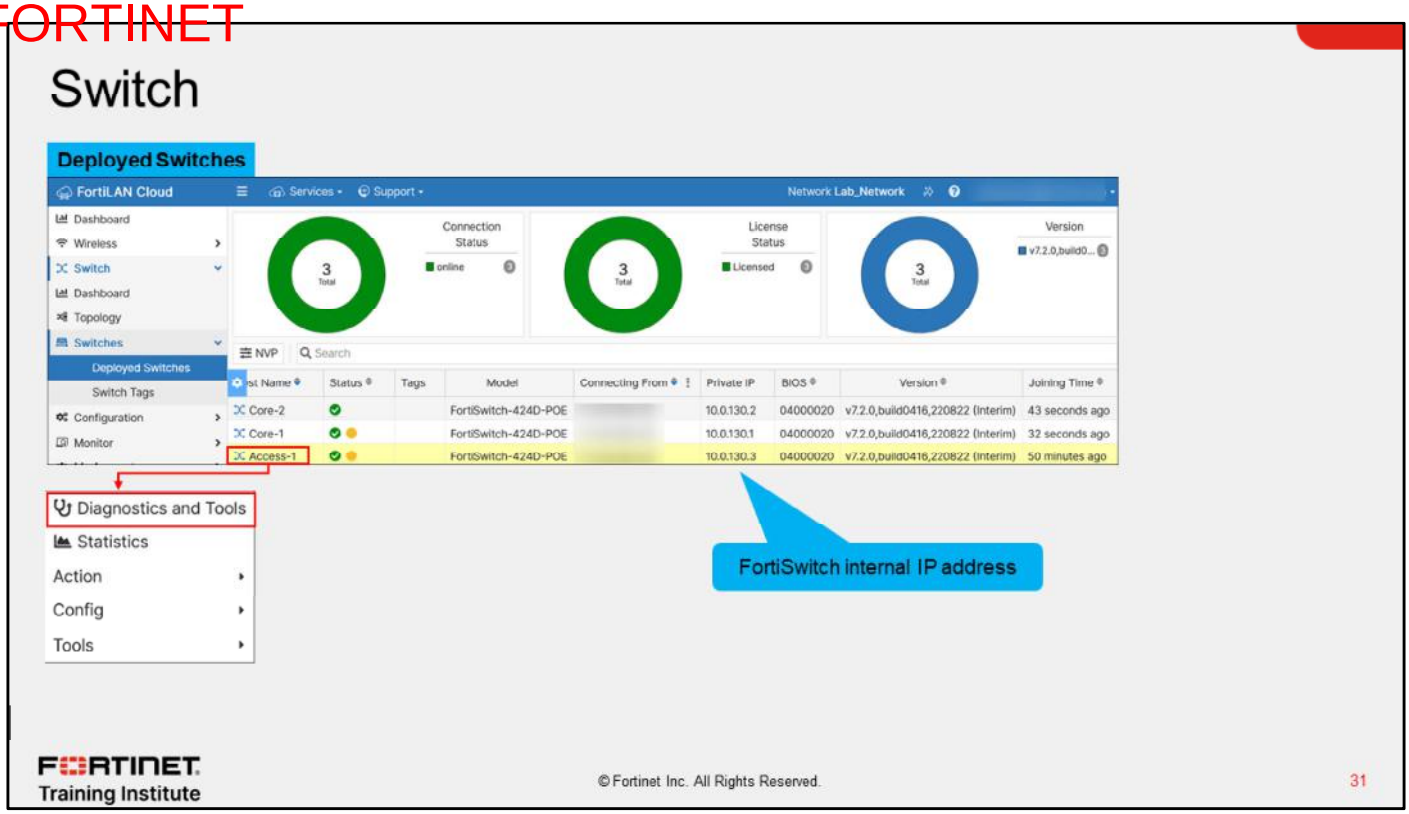
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Detail Topology** page displays the ports that connect to each LLDP neighbor. Click a device in the topology to display the details. The example on this slide shows the connection details for the FortiSwitch device named Core-1.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

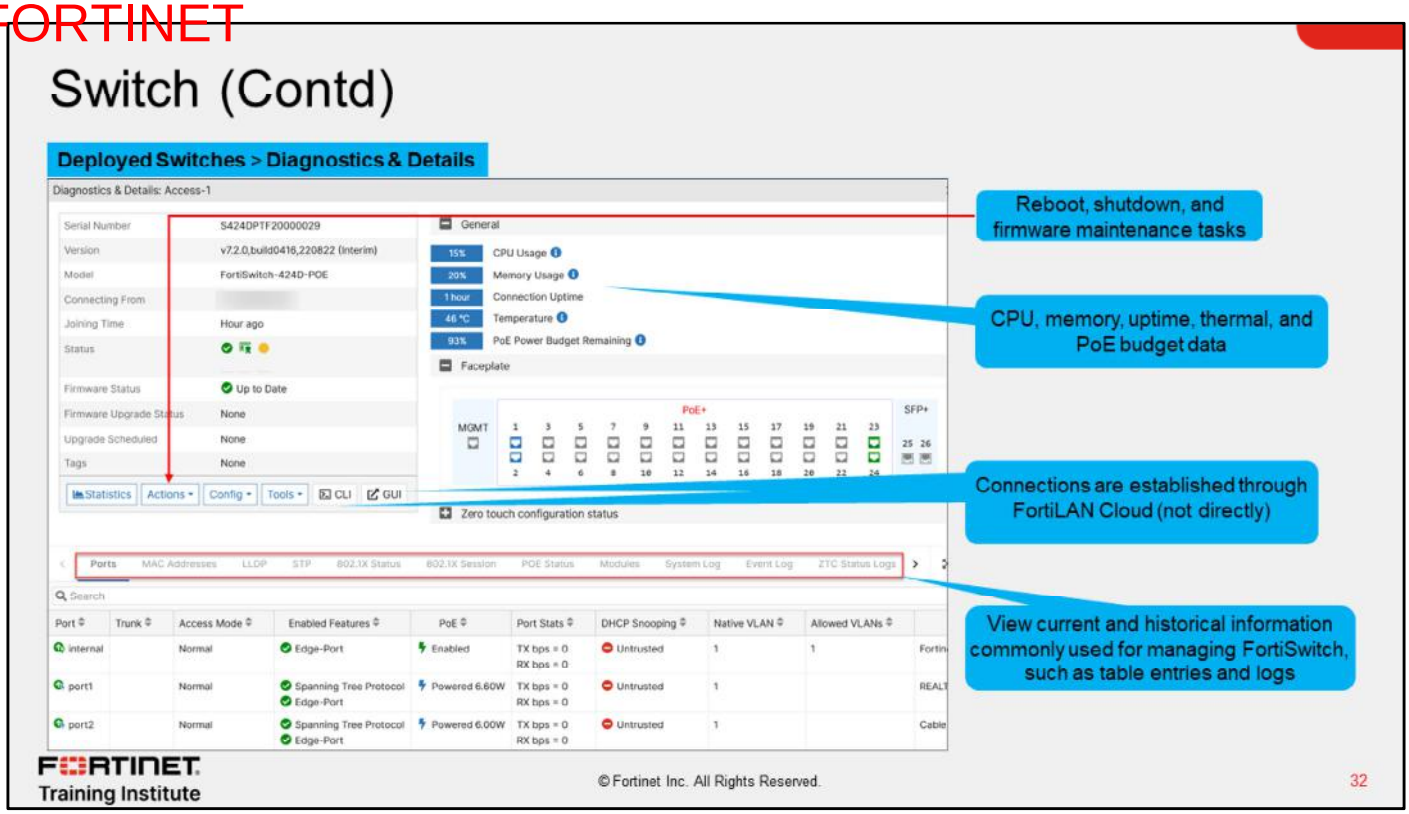


The **Deployed Switch** page provides you with a list of the FortiSwitch devices that are currently being managed on FortiLAN Cloud.

Right-click a switch to display a list of available actions and information. You can also click the graph icon in the **Action** column to display historical graphs for important operating parameters, such as CPU, temperature, bandwidth, and the number of entries in the MAC address table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

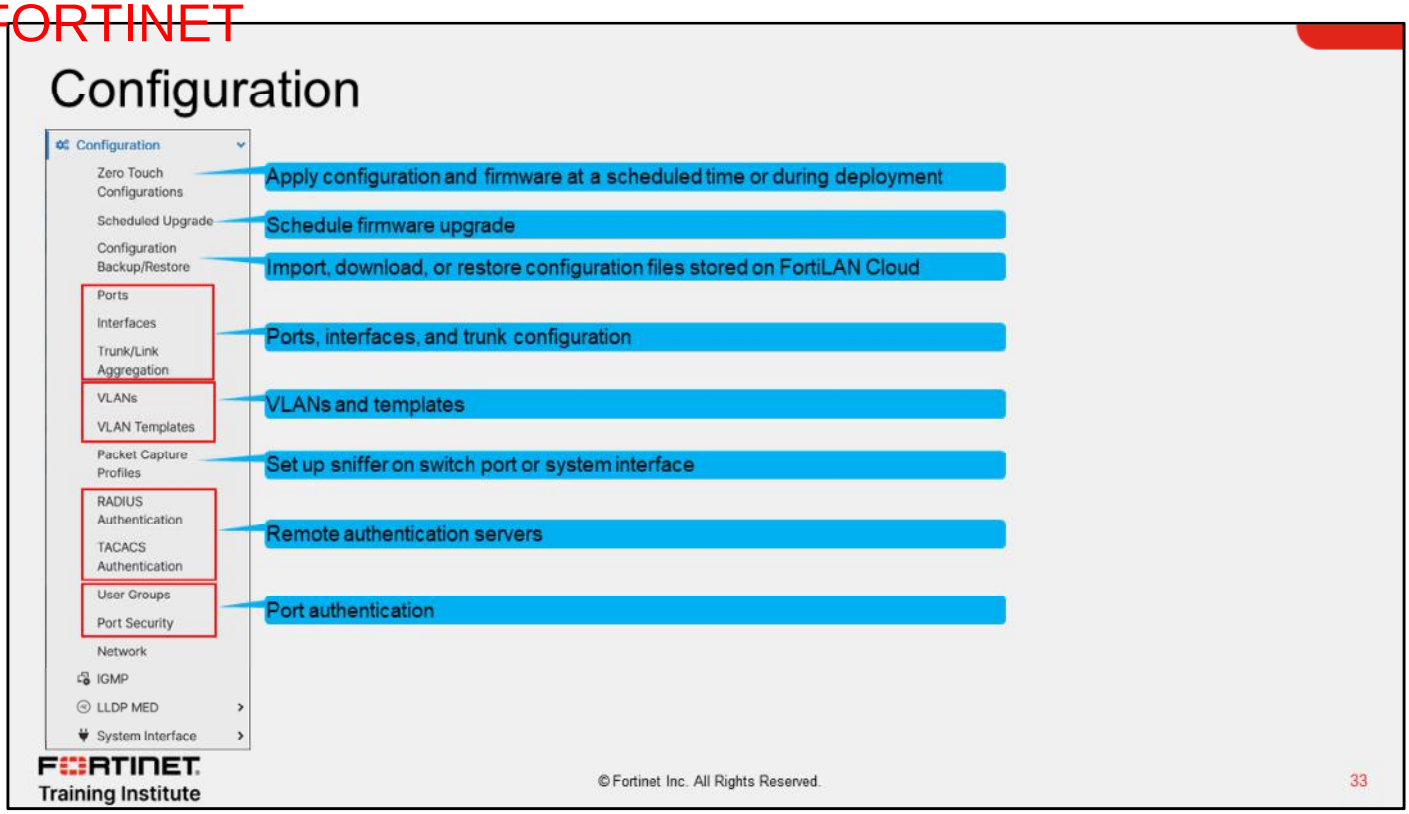


The **Diagnostics & Details** page enables you to perform many common configuration and maintenance tasks, such as configuration backup and restore, rebooting the switch, viewing switch port details, and firmware upgrade. You can also initiate cable tests, initiate ping and traceroute diagnostics, bounce physical ports, reset PoE, view the MAC address table, routing table, LLDP neighbor details, and so on.

This page also provides you with SSH and GUI connection tools. When you connect to the FortiSwitch GUI or CLI using FortiLAN Cloud, you establish a secure connection to the device through FortiLAN Cloud, not directly.

Vouchers & Dumps are Available | WhatsApp +201224560923

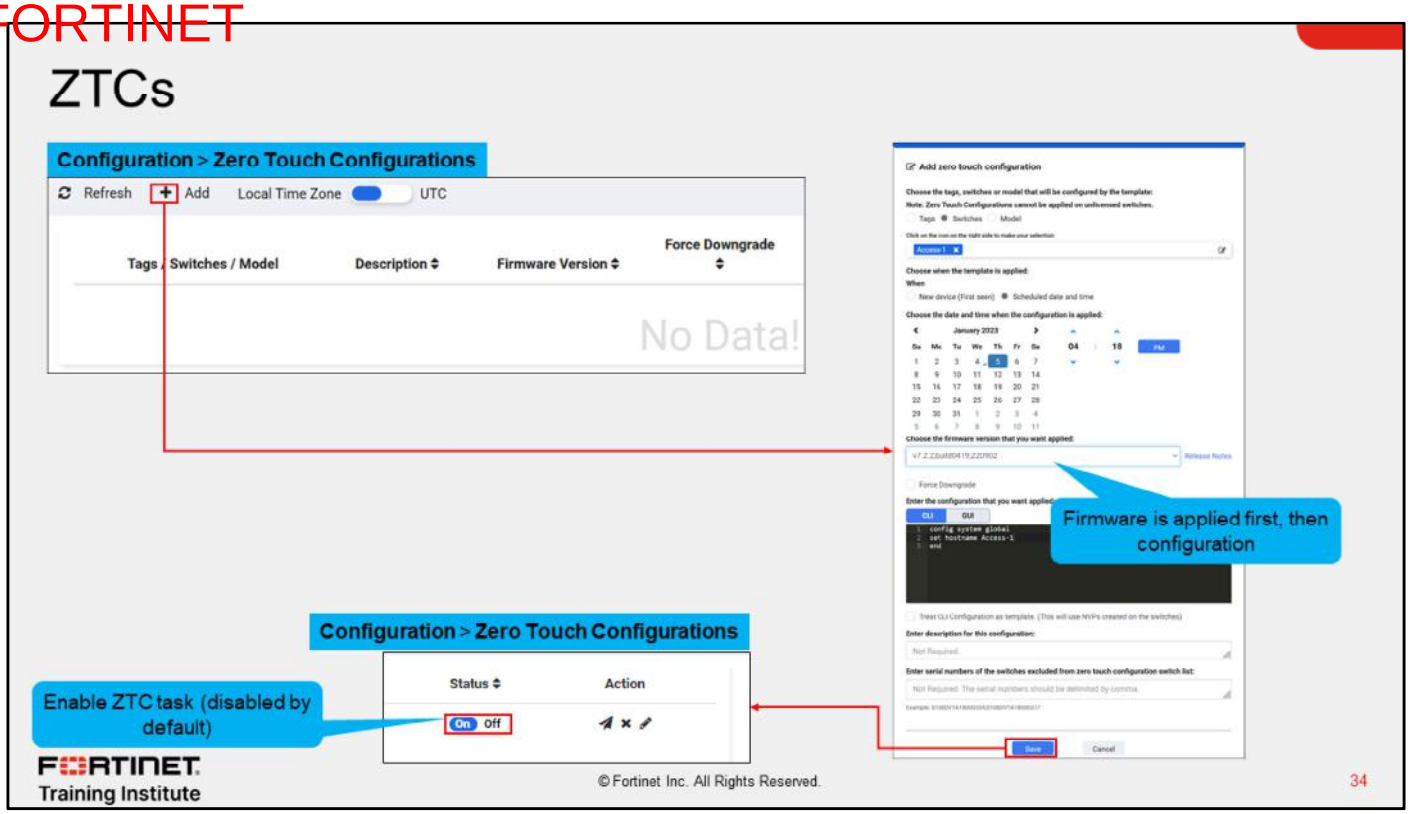
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Configuration** page displays configuration tools for the most common features on FortiSwitch. Most of the features shown here should be familiar to you already, and the way to configure them is very similar to how you would configure them on a FortiGate-managed switch or on FortiSwitch directly. For this reason, the lesson focuses on the first three features only, which are unique on FortiLAN Cloud: **Zero Touch Configurations**, **Configuration Backup/Restore**, and **Scheduled Upgrade**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Zero touch configurations (ZTCs) enable you to apply configuration settings and firmware to one or more switches at a scheduled time, or when the switch connects to FortiLAN Cloud for the first time. You can select the target switches by tag, serial number, or model.

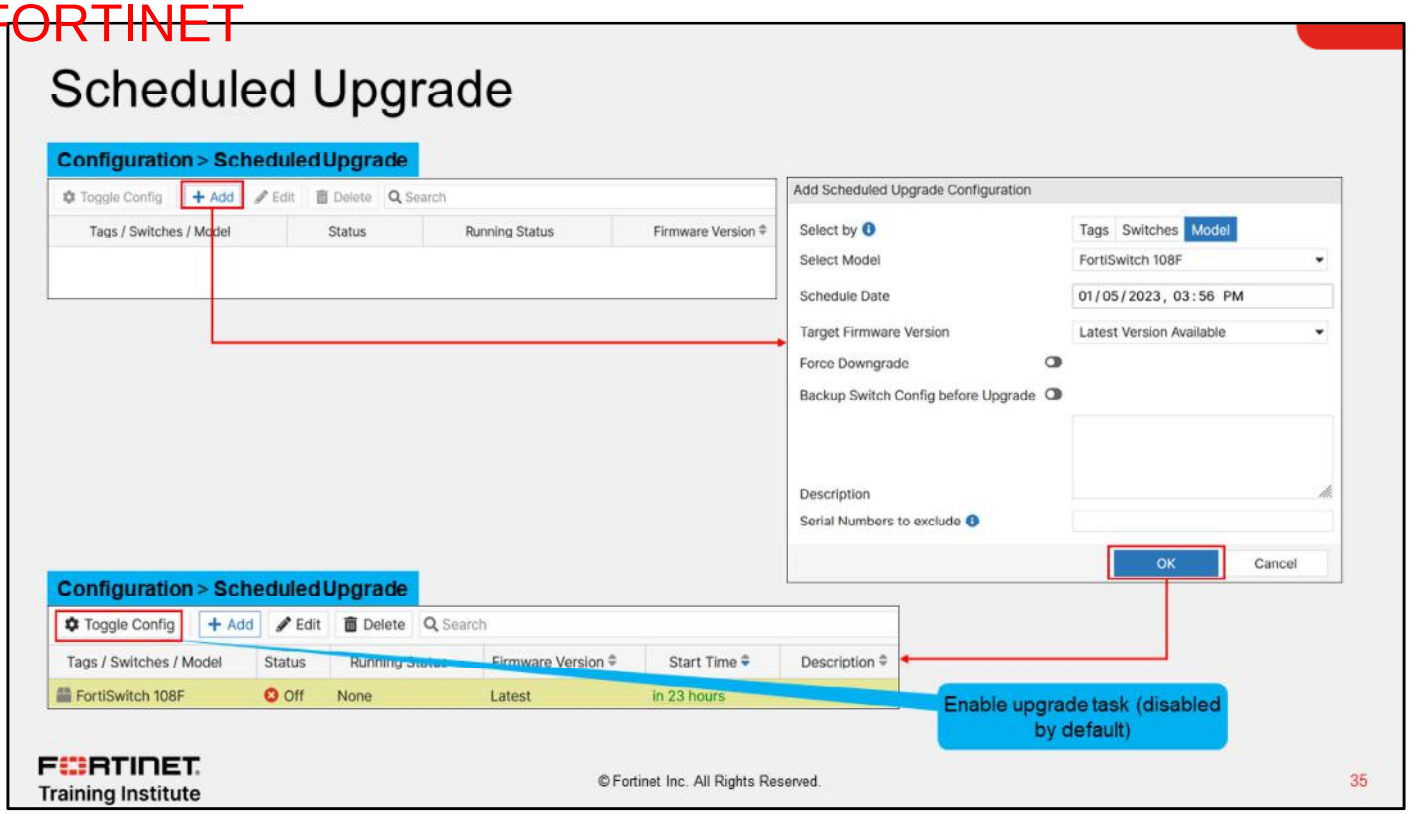
To apply a configuration using ZTCs, you enter the corresponding FortiSwitchOS CLI settings you want to run on the device. If you also select a firmware version for the device, then FortiLAN Cloud first applies the new firmware on FortiSwitch, and then applies the configuration.

New ZTC tasks are disabled by default. Therefore, you must enable the task by toggling the task status button on the ZTCs page.

The example on this slide shows a ZTC task that applies the firmware version 7.2.2 to the switch, and sets its hostname. The switch is selected by hostname, and the task is scheduled to run at a specific date and time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



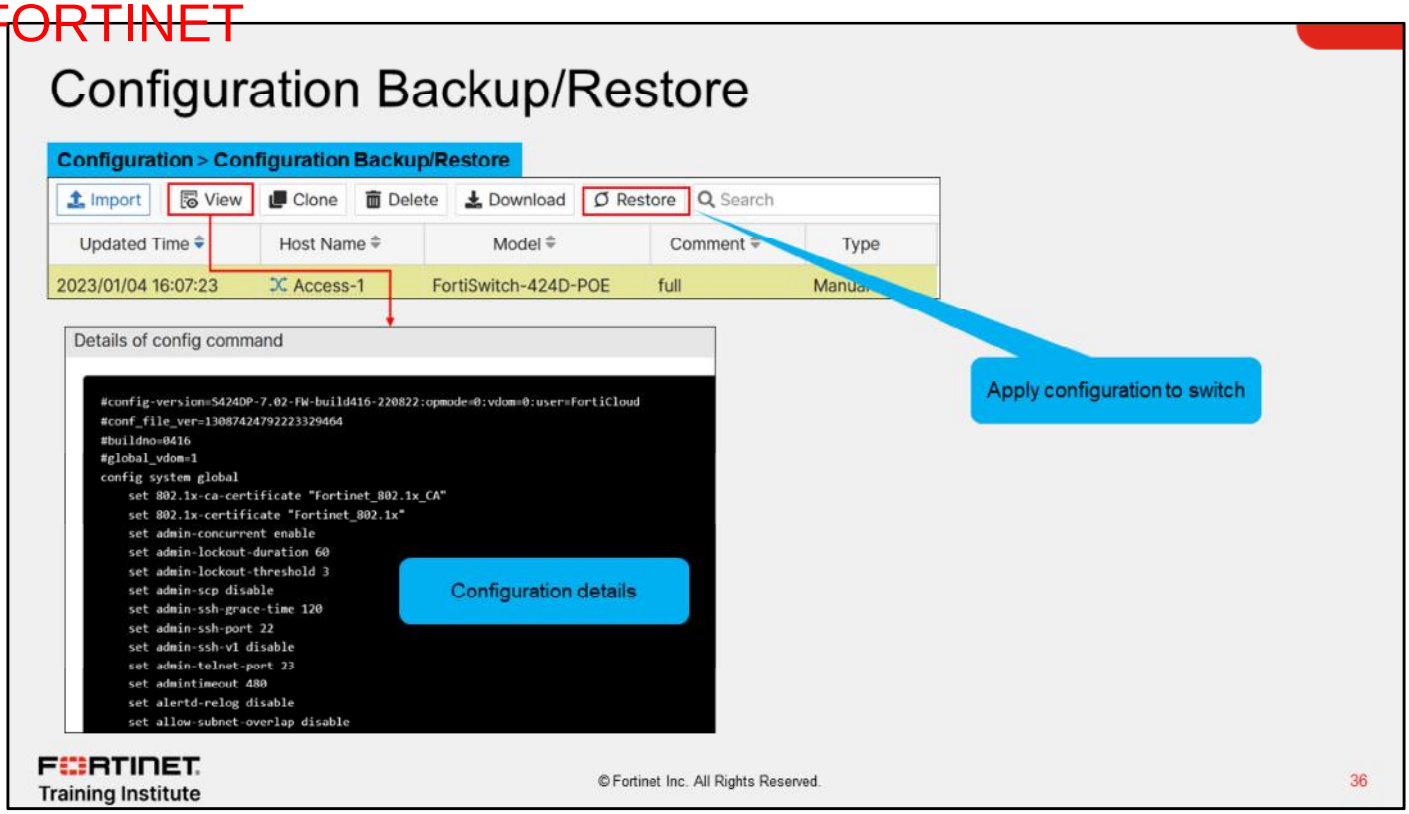
Browse to the **Scheduled Upgrade** page to schedule firmware upgrades on one or more switches. You can select the target switches by model, tag, or hostname.

New scheduled upgrade tasks are disabled by default. Therefore, you must enable the task by toggling its status button.

The example on this slide shows a scheduled upgrade task that applies the latest firmware version available to all 108F model FortiSwitches. The switches are selected by model number and the task is scheduled to run at a specific date and time. Note there is a field available where you can add serial numbers to exclude specific devices from the upgrade process.

Vouchers & Dumps are Available | WhatsApp +201224560923

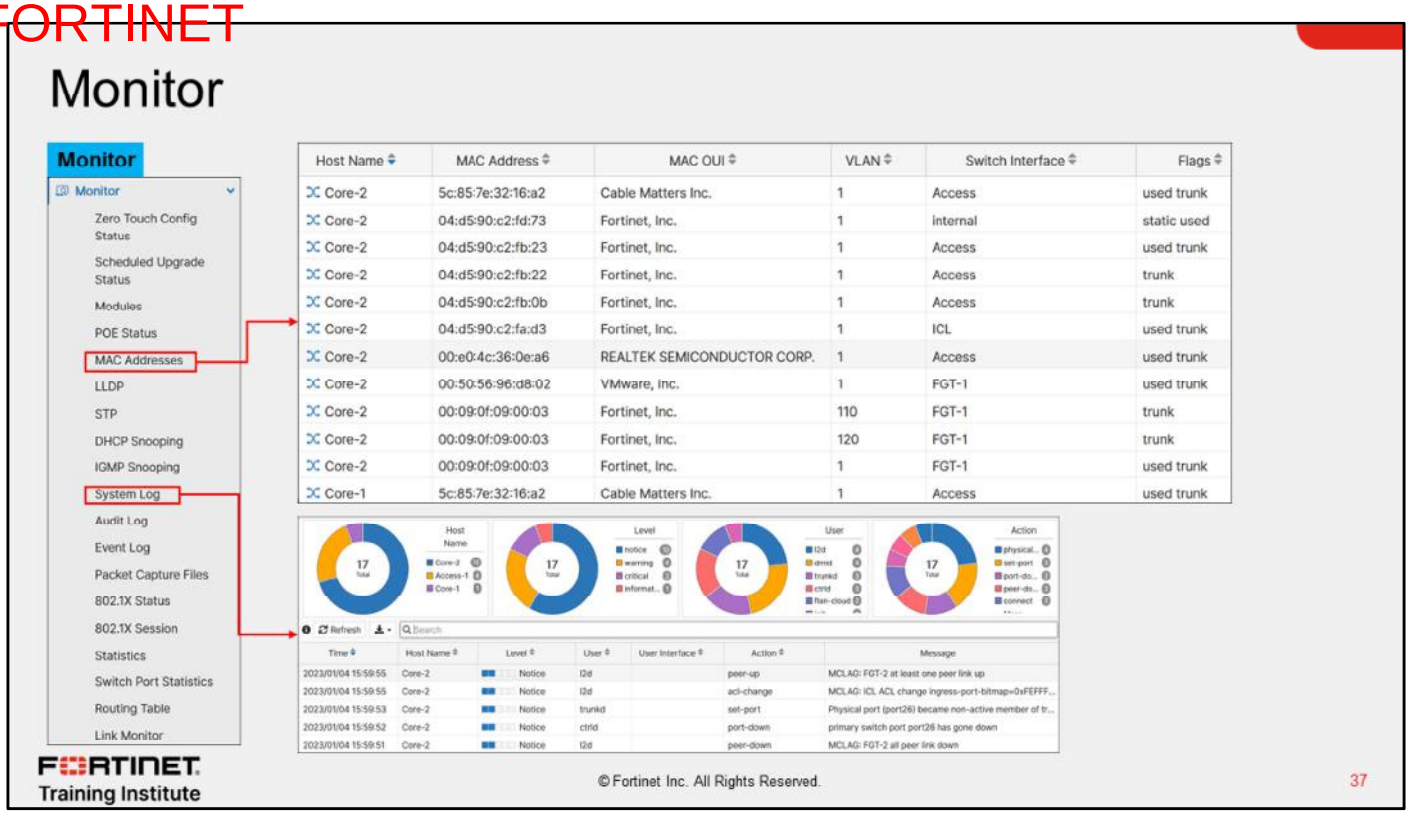
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Configuration Backup/Restore** page enables you to import, clone, and restore to FortiSwitch a configuration file stored in FortiLAN Cloud. You can quickly review the contents of the configuration file by clicking the **View** button. If you want to apply the configuration to the switch, click the **Restore** button while the desired configuration is selected, as shown on this slide. Note that applying the configuration to a switch causes the switch to reboot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Browse to the **Monitor** page to view the status of the most common features. This slide shows sample screenshots for some of the features you can monitor. Note that although the information displayed is for all managed switches, you can filter information for a particular switch, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about FortiLAN Cloud operation is true?
   - ✓ A. FortiLAN Cloud is disabled by default.
   - B. FortiSwitch uses HTTP to connect to FortiLAN Cloud.

2. What information does FortiLAN Cloud use to build its topology?
   - A. Entries in the MAC address table
   - ✓ B. Entries in the LLDP neighbor table

3. Which statement about ZTCs is true?
   - A. Tasks can be configured to run only when FortiSwitch connects to FortiLAN Cloud for the first time.
   - ✓ B. The firmware is applied first, and then the configuration.

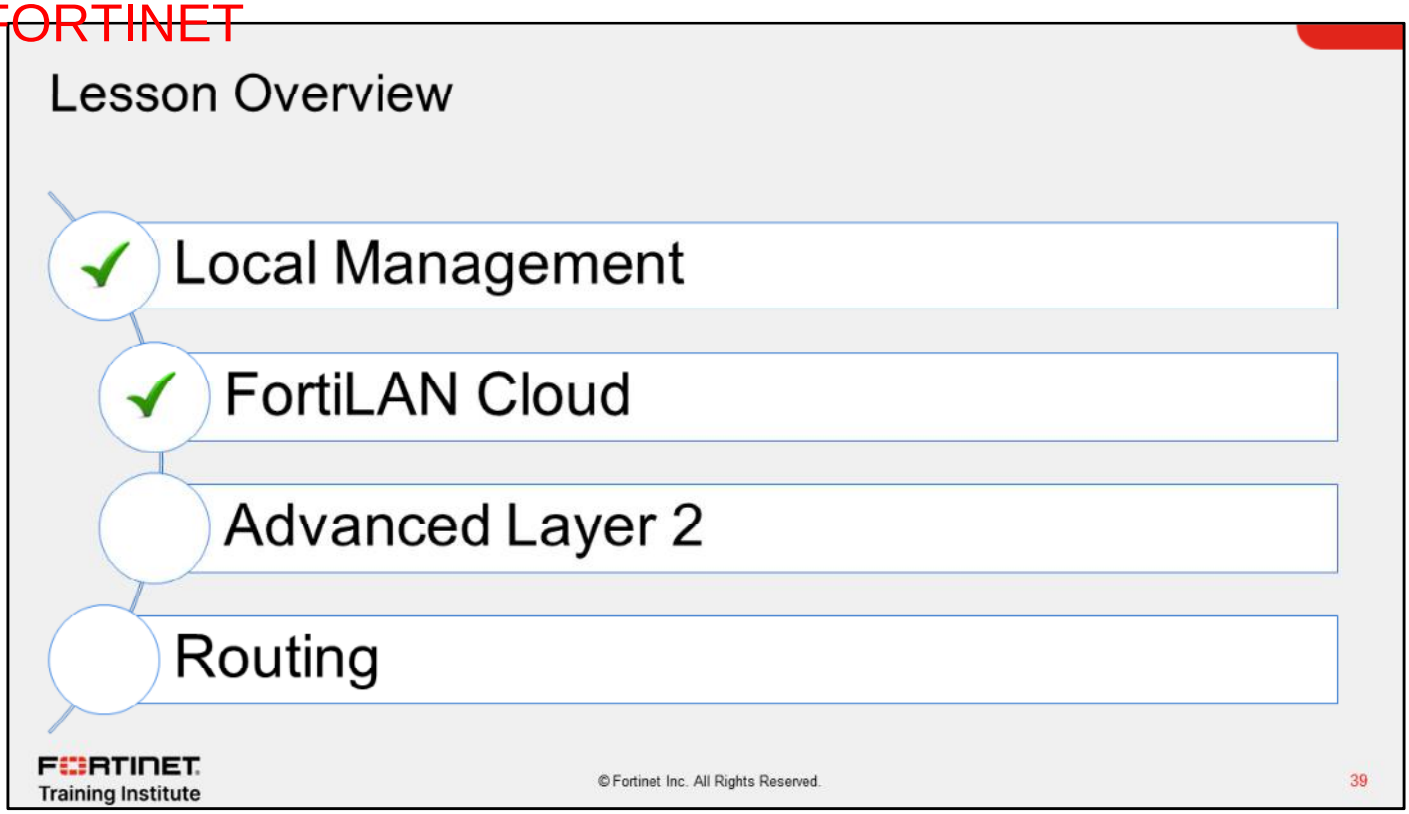
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

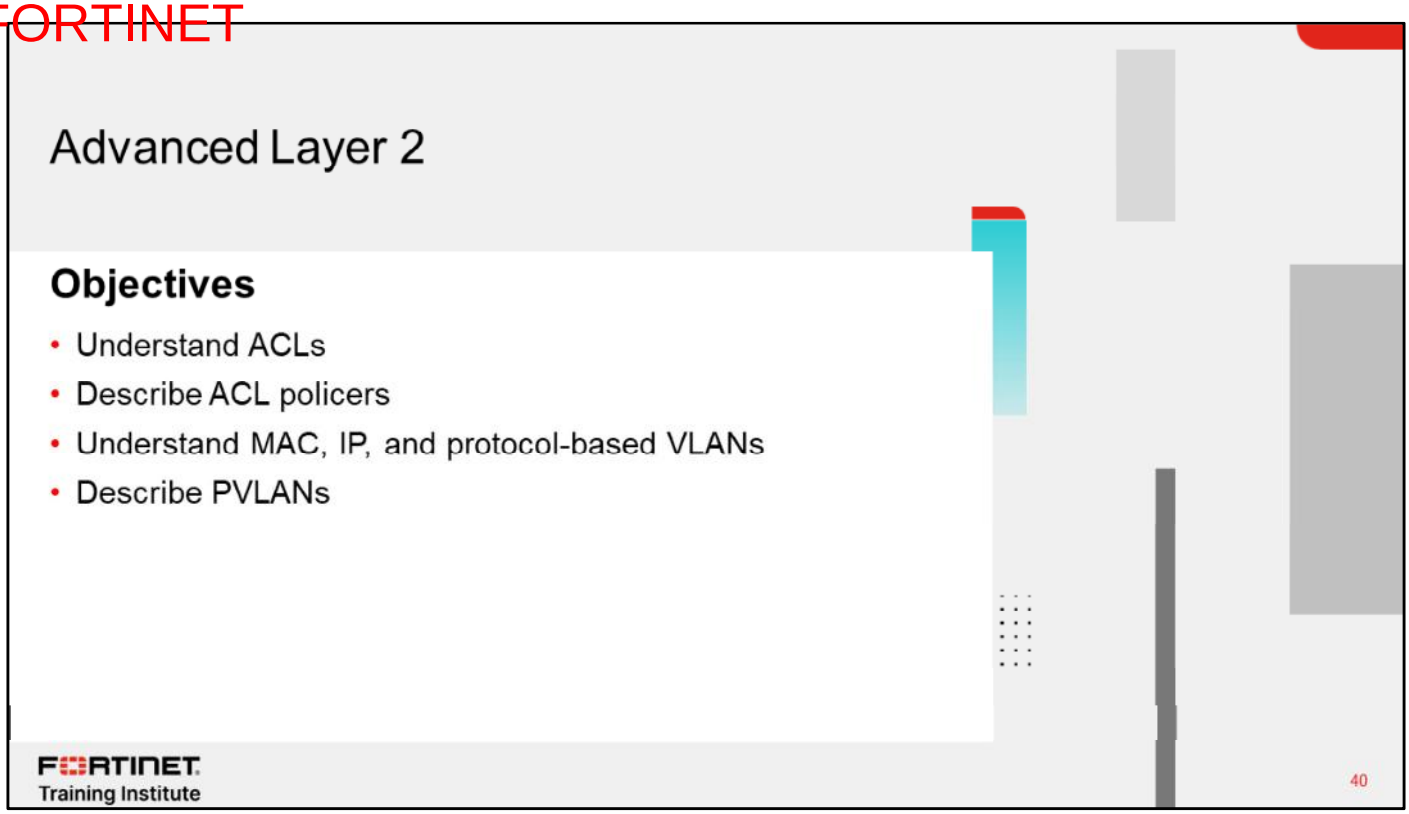


Good job! You now understand FortiLAN Cloud.

Now, you will learn about advanced Layer 2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

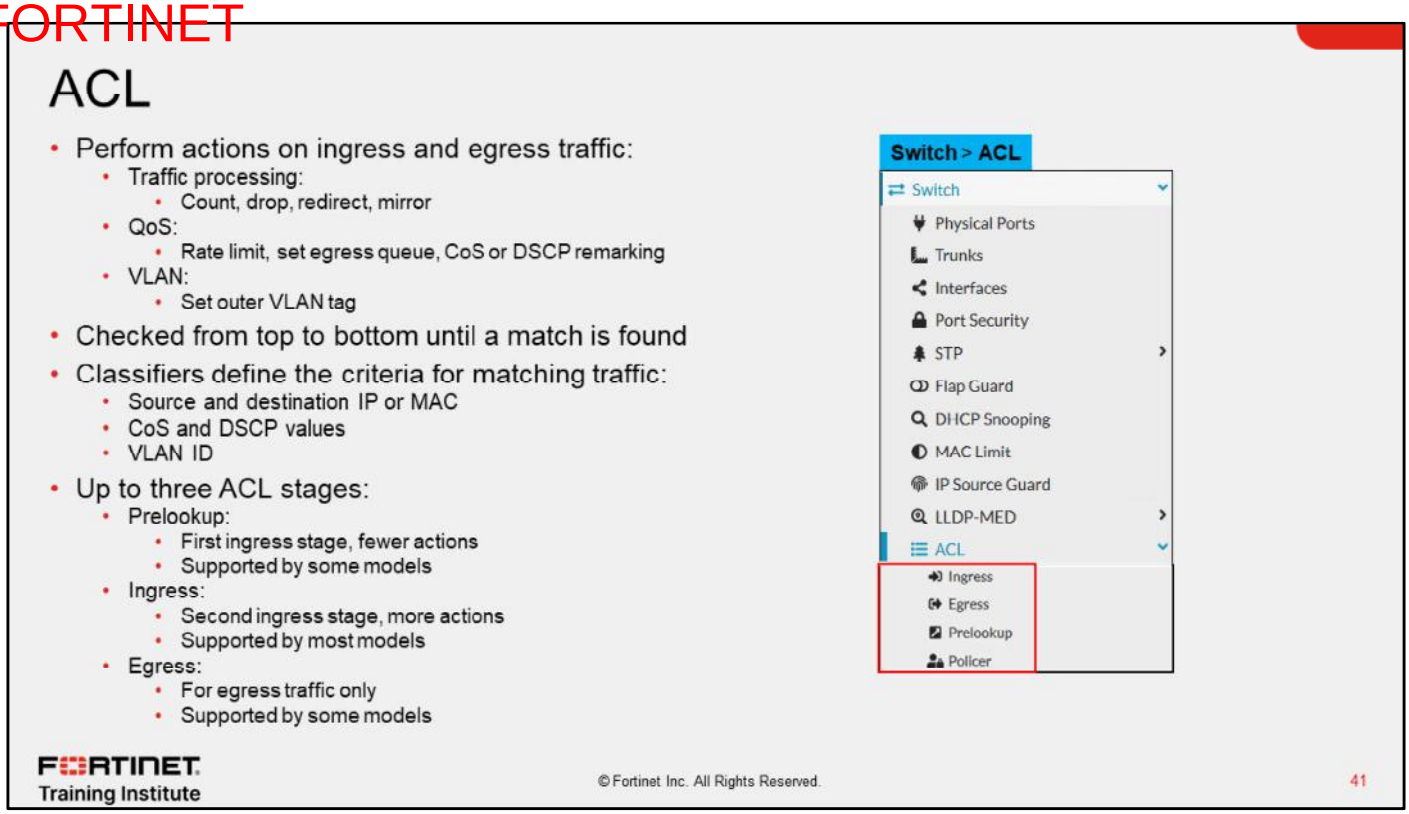


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in advanced Layer 2, you should be able to understand how to use ACLs, MAC, IP, and protocol-based VLANs, and PVLANs to deploy sophisticated Layer 2 services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Access control lists (ACLs) enable you to perform multiple actions on matching traffic that enters and leaves the switch. You can configure FortiSwitch to perform the following type of actions on traffic:

- Traffic processing: count, drop, redirect, or mirror frames
- QoS: rate limit, set egress queue, or remark CoS and DSCP values on frames
- VLAN: set outer VLAN tag on frames

To match traffic on ACLs, you configure classifiers. Classifiers enable you to match traffic using multiple criteria such as: destination and source IP addresses, destination and source MAC addresses, CoS and DSCP values, and VLAN ID. FortiSwitch checks ACL policies from top to bottom until it finds a match.

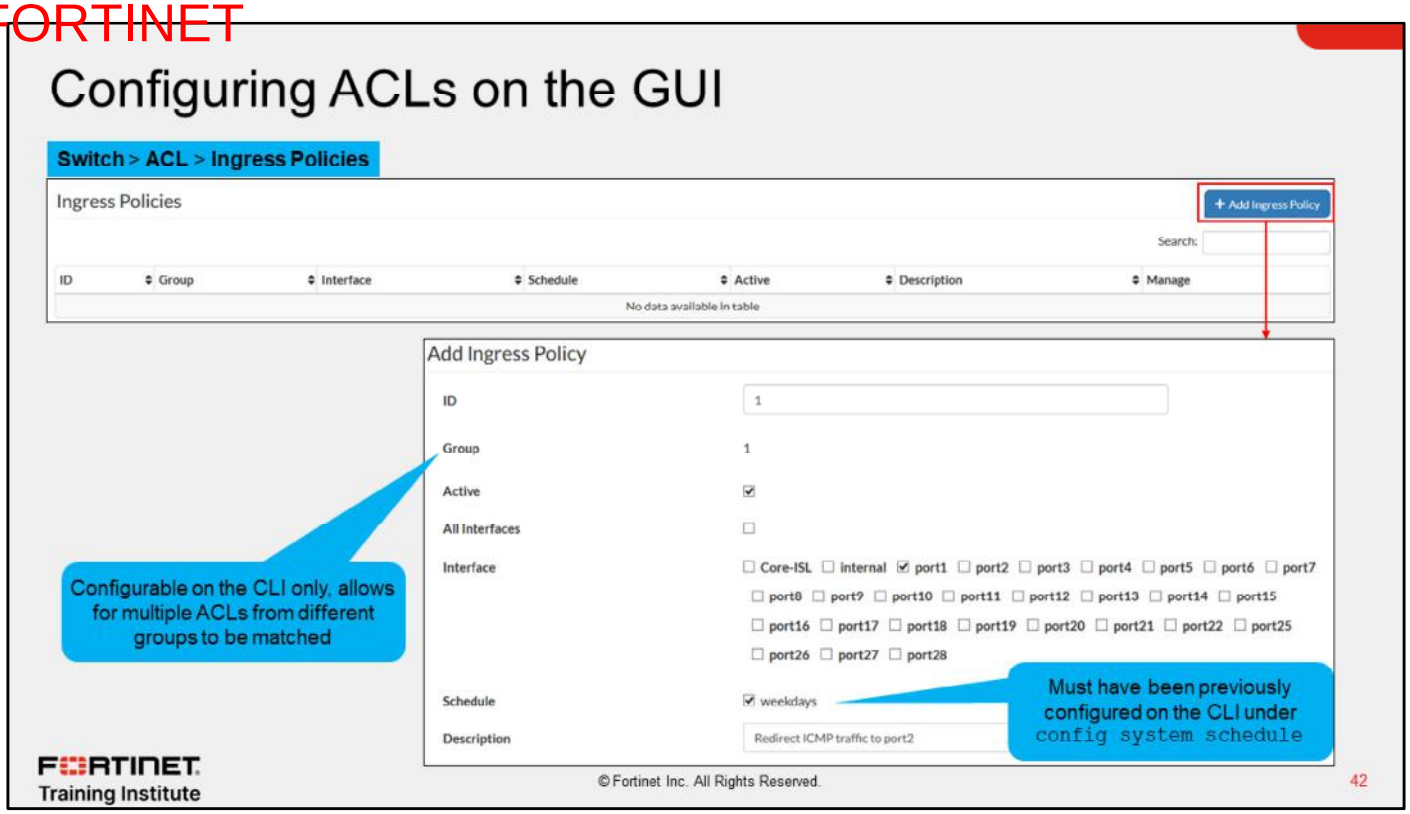
You can configure ACLs at different stages of the traffic processing pipeline. Depending on the FortiSwitch model, there are up to three different stages you can configure ACLs on:

- Prelookup: This is the first stage in the pipeline for ingress traffic. It takes place before the switch performs Layer 2 and Layer 3 lookups, and it supports a reduced number of actions. If the action you need is supported on this stage, then in most cases, it is better to apply the action at this stage, before the switch handles the traffic any further.
- Ingress: This is the second stage for ingress traffic. It supports a higher number of actions.
- Egress: Actions are applied on egress traffic only.

Most FortiSwitch models support ACLs at the ingress stage. However, only some models support ACLs at the prelookup and egress stages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the first part of an ACL ingress policy configuration that redirects ICMP traffic received at port1, to port2. The procedures to create ACL prelookup and egress policies are the same except that you have fewer options available for classifiers and actions.

The first step during an ACL configuration is to indicate the ACL policy ID and the interfaces to apply the ACL policy on. The example on this slide shows **port1** as the selected interface, which means that the ACL ingress policy is applied on the ingress traffic received at port1. Optionally, you can also select an ACL group and a schedule.

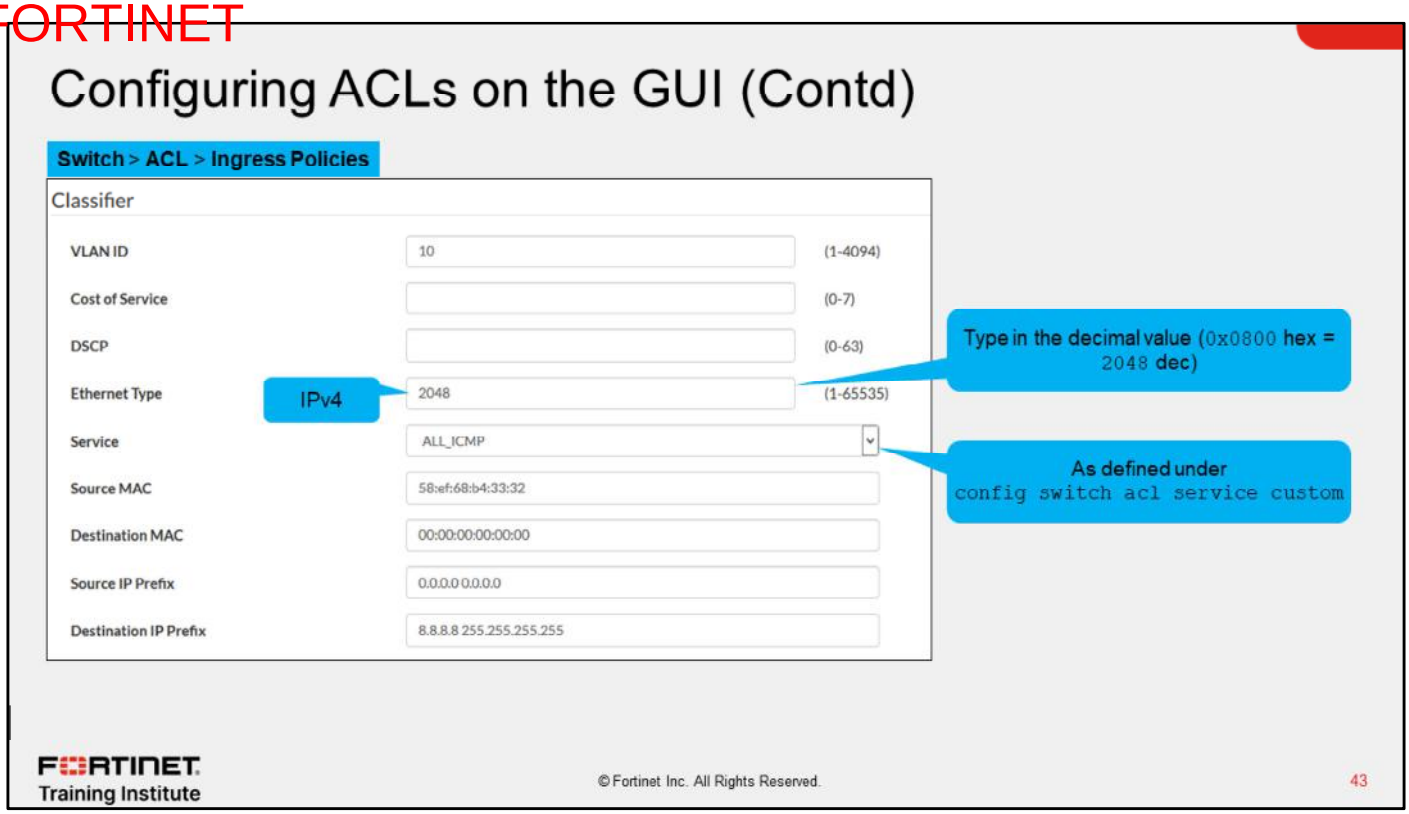
ACL groups allow the same packet to match multiple ACL policies by arranging ACL policies in groups. The result is that FortiSwitch checks in parallel the ACL policies configured in multiple groups, and then applies the non-conflicting actions configured on each matching ACL. If there is a conflicting action, FortiSwitch resolves it by applying the action of the ACL with the lowest group number.

The number of supported ACL groups is platform dependent. For example, a FortiSwitch 224E model supports four groups. By default, all ACL policies configured on the GUI are placed in group 1. If you want to set a different group on an ACL, then you *must* set the group using the CLI and when you create the ACL.

Schedules indicate the days and times to enforce the ACL on. For FortiSwitch to display the schedules on the GUI, you must have previously configured them using the FortiSwitch CLI under `config system schedule`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



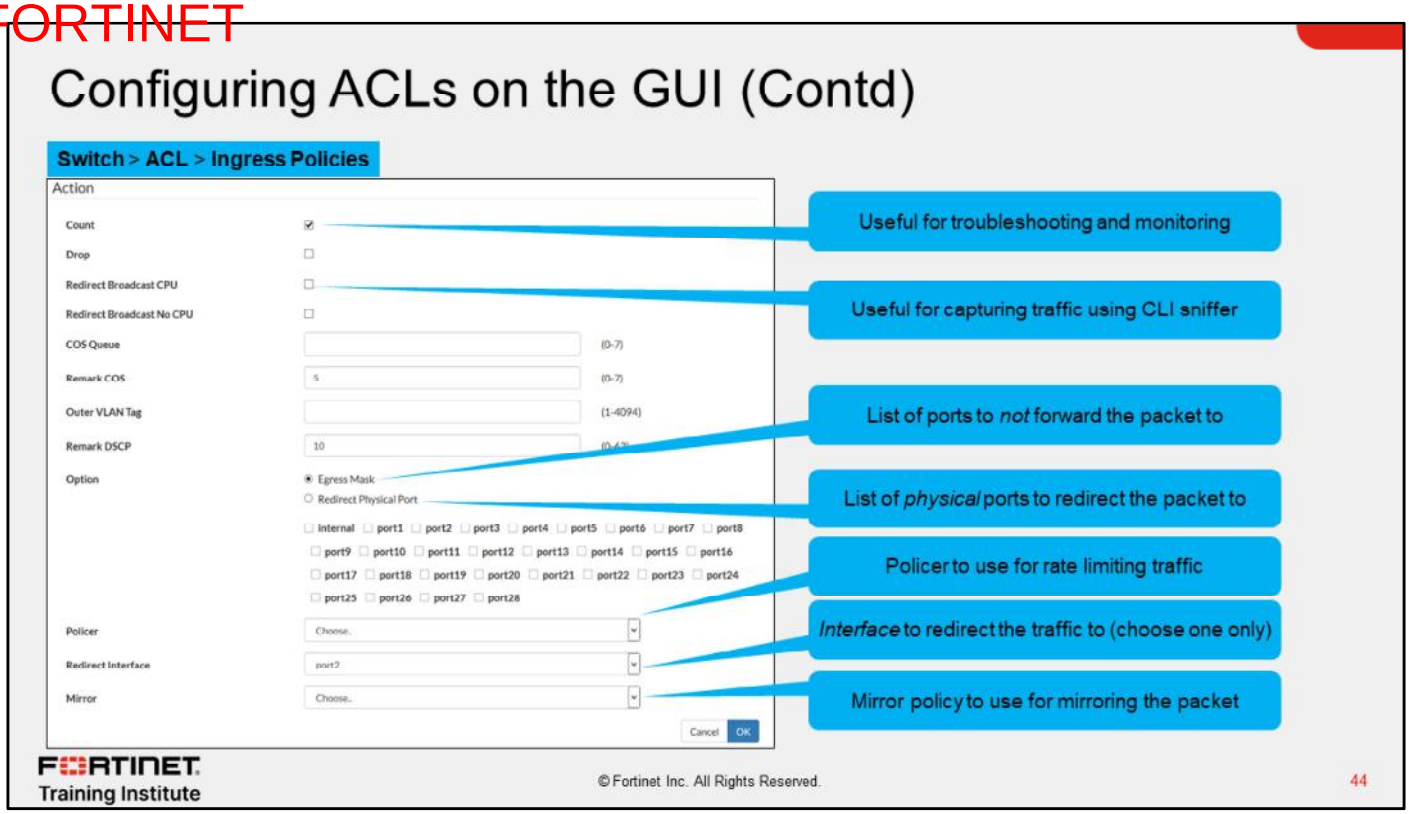
This slide shows the second part of an ACL ingress policy configuration, specifically the **Classifier** section. Here, you set the criteria that FortiSwitch looks for on the packet to determine a match. You can define multiple Layer 2 and Layer 3 criteria.

You can also define the service to match—all ICMP traffic in the example. FortiSwitch comes with a list of predefined services. If your traffic doesn't match any of the predefined services, you can configure a custom service on the CLI under `config switch acl service custom`.

Note that the **Ethernet Type** field requires you to type the Ethernet type value in decimal. For example, IPv4, which is `0x0800` in hexadecimal, equals to `2048` in decimal.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



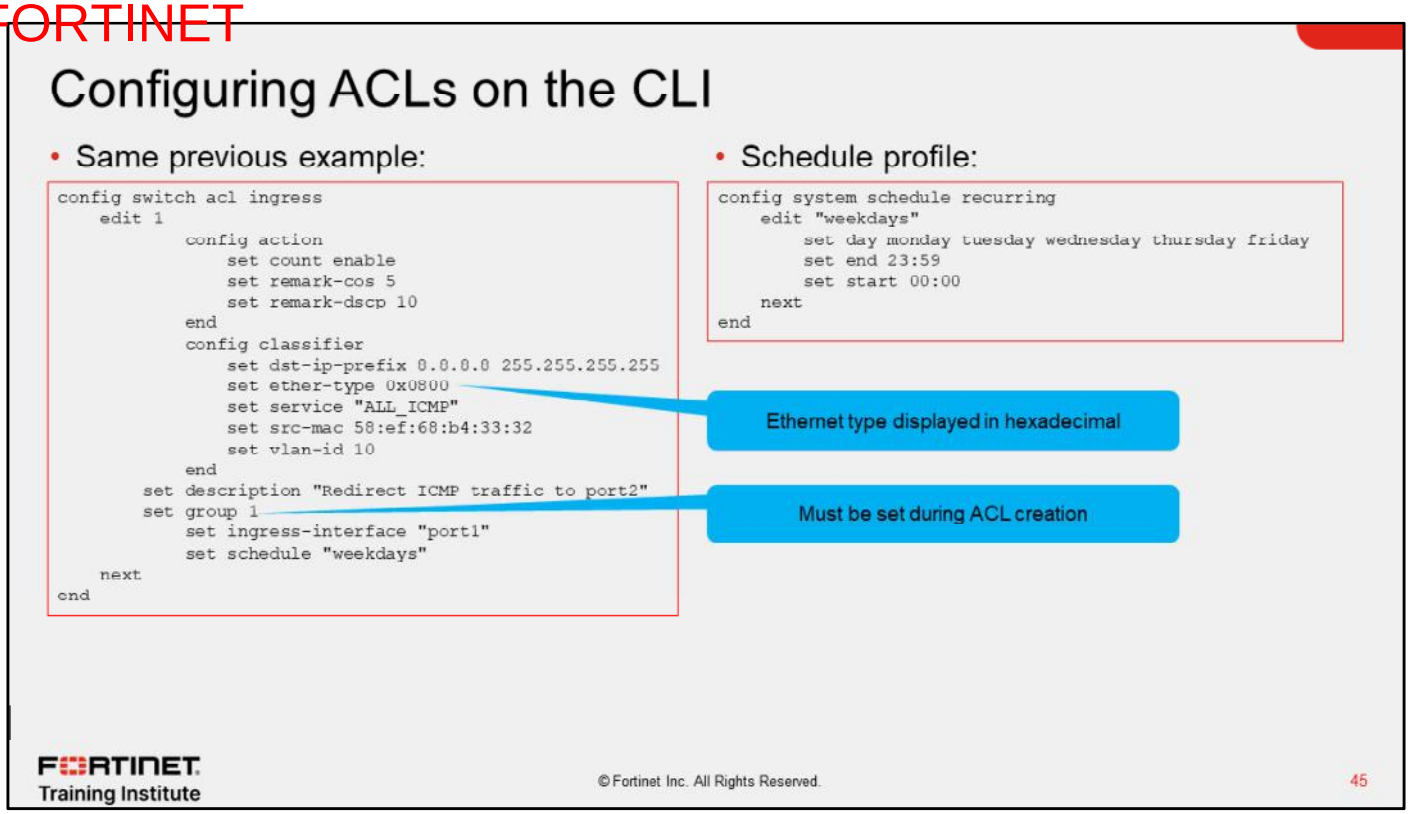
This slide shows the last part of an ACL ingress policy configuration, specifically the **Action** section. There are multiple actions to choose from, and they vary among stages. The example on this slide instructs FortiSwitch to count matching packets and remark them with `5` and `10` as the CoS and DSCP values, respectively. In addition, the packet is forwarded to **port2**. Counting packets is useful for troubleshooting and monitoring purposes, because sometimes you want to know if a port received a packet that matches a specific classifier on the ACL policy.

There are three options that control how matching packets are forwarded. **Egress Mask** indicates the ports the packet must *not* be forwarded to, while **Redirect Physical Port** indicates a list of *physical* ports to redirect the packet to. You can also use the **Redirect Interface** option, which is similar to **Redirect Physical Port**, except that you can also redirect packets to logical interfaces, such as the internal interface and trunks, and not just to physical ports. A downside of using **Redirect Interface** is that you can select one interface only, whereas **Redirect Physical Port** allows you to select multiple ports. Note that you can't use **Egress Mask** or **Redirect Physical Port** options at the same time as **Redirect Interface**.

Another two actions available are mirroring and policing. Mirroring enables FortiSwitch to send a copy of the matching packet to a monitoring device by using SPAN, RSPAN, or ERSPAN, as defined in the selected **Mirror** profile. The original packet is still processed according to the forwarding rules configured on the port (drop, count, redirect, and so on). It is just that a copy of the packet for monitoring and troubleshooting purposes is made. You will learn more about mirroring in another lesson. Policing enables FortiSwitch to rate limit the traffic based on the selected **Policer** profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

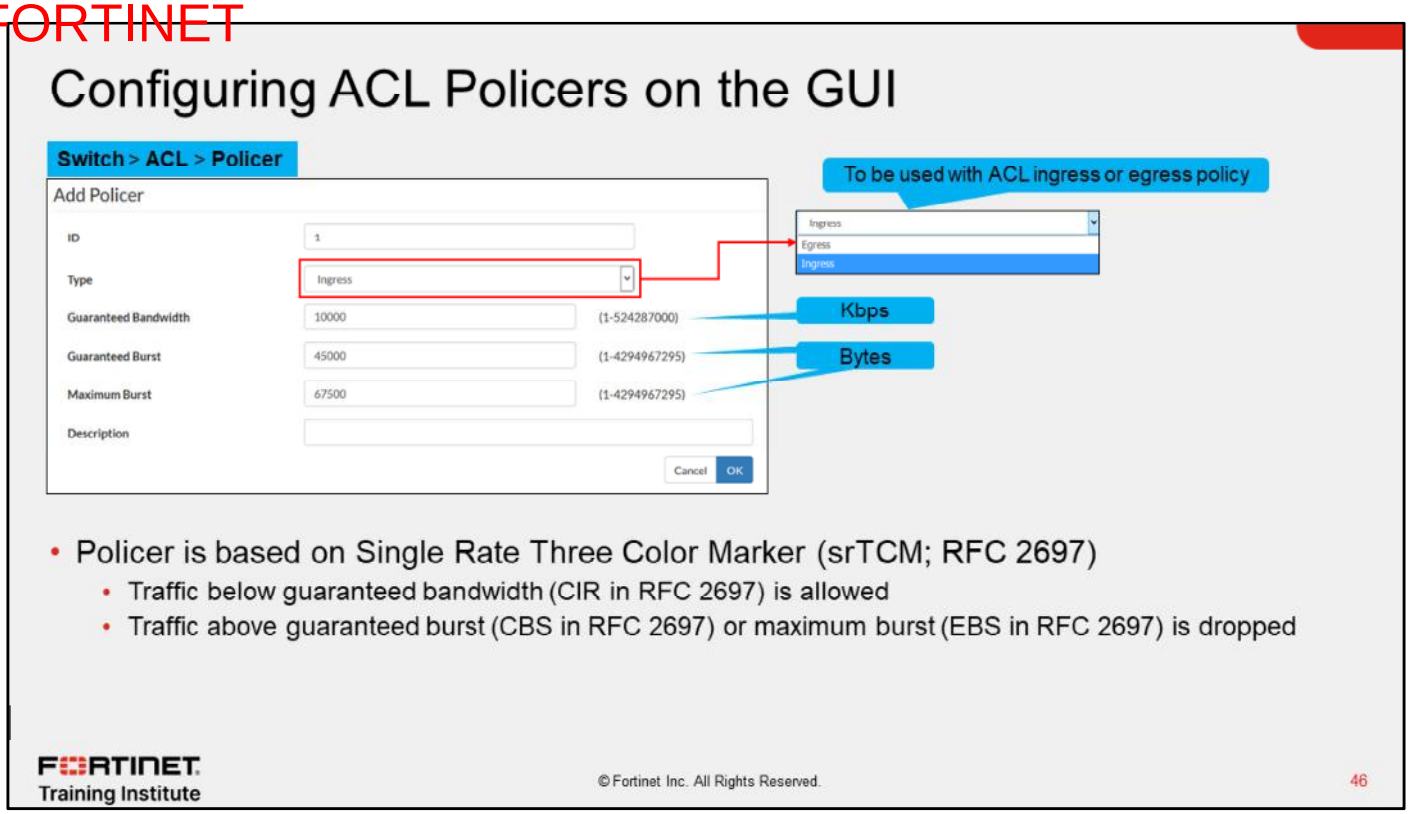


This slide shows the equivalent CLI settings for the ACL ingress policy that was previously configured on the GUI. Note that the CLI shows the Ethernet type in hexadecimal. This slide also shows the settings for the schedule selected on the ACL ingress policy.

In addition, remember that if you want to assign the ACL policy to a different group (the default group is `1`), then you must set the group ID on the CLI and during ACL creation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



ACL policers enable you to rate limit the traffic that matches an ACL policy. The policer implementation is based on the Single Rate Three Color Marker (srTCM; RFC 2697).

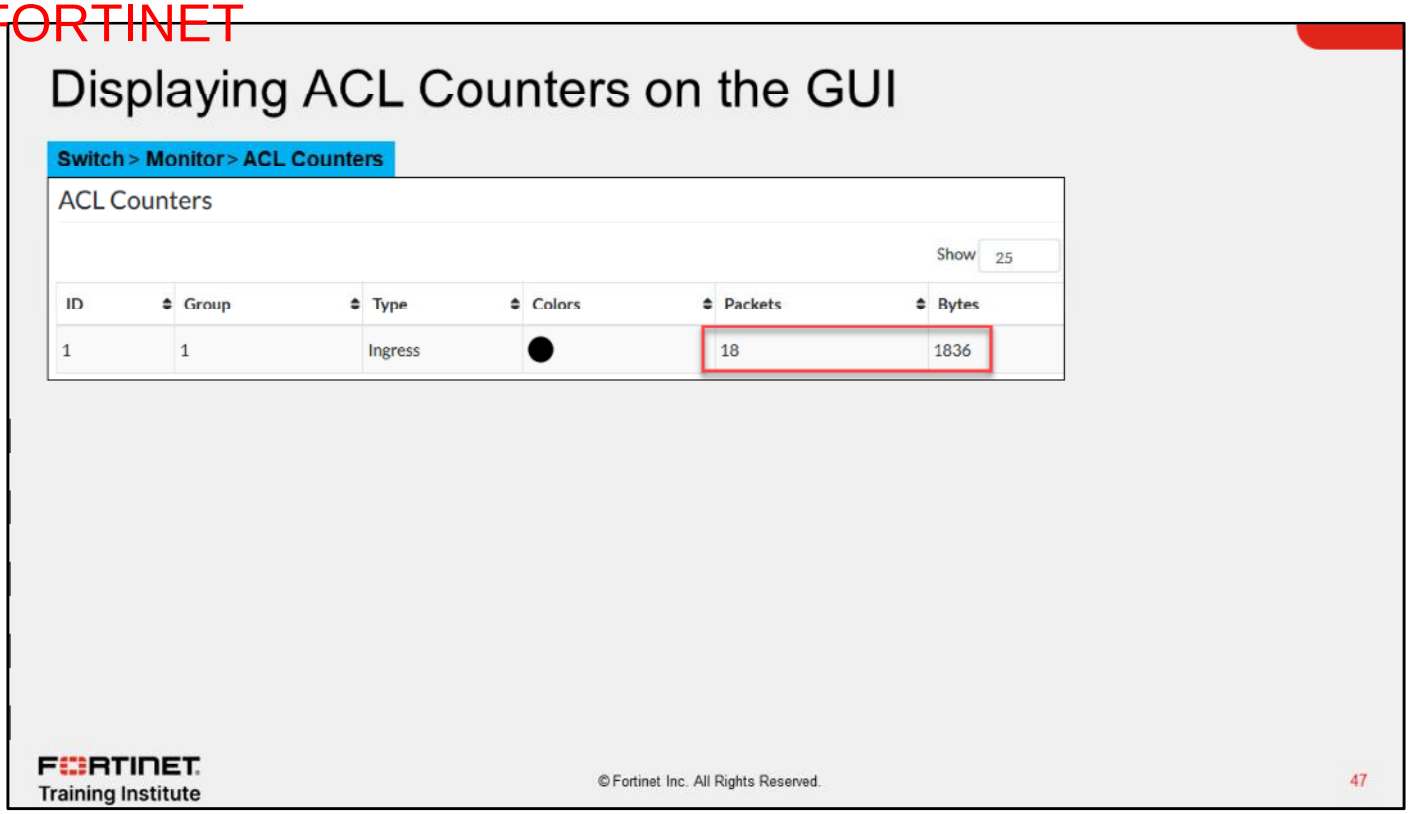
The **Guaranteed Bandwidth**, **Guaranteed Burst**, and **Maximum Burst** settings correspond to the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS) parameters defined in RFC 2697, respectively.

Traffic below the guaranteed bandwidth is marked green. Traffic above the guaranteed burst and below the maximum burst is marked yellow. Traffic above the maximum burst is marked red. FortiSwitch then allows traffic marked as green, and drops traffic marked as yellow or red.

This slide shows an example of an ACL policer configuration. Note that the **Type** setting determines whether the policer is to be used on an ACL ingress policy or on an ACL egress policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



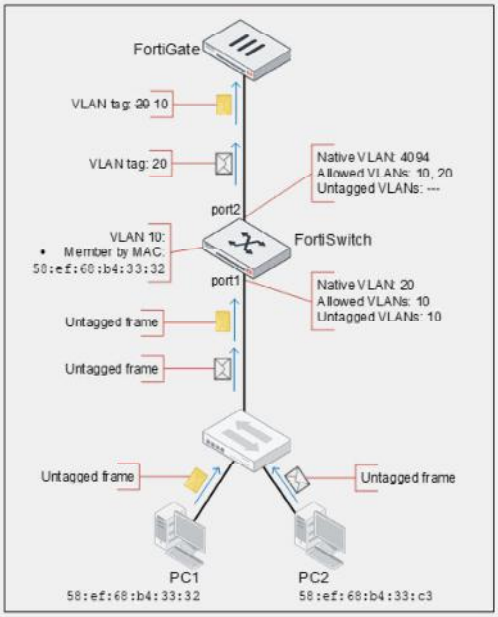
If you enable the count action on the ACL policy, then FortiSwitch counts every packet that matches the ACL classifier. You can browse to the **ACL Counters** page to display the total number of matching packets and bytes on the ACL.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MAC, IP, and Protocol-Based VLANs

- Assign members to VLANs based on their:
  - Source MAC address
  - Source IPv4/IPv6 address
  - Ethernet protocol
- Port VLAN settings are overridden for ingress traffic
- Benefits:
  - Devices behind same switch port can be on different VLANs
  - Endpoint mobility
    - Bound VLAN remains the same regardless of port
      - Not scalable and secure
      - Dynamic VLAN assignment over 802.1X is preferred



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

Usually, you assign ports to VLANs by configuring the native VLAN and allowed VLAN settings on the port. FortiSwitch then uses these settings to determine the VLAN to assign untagged and tagged ingress traffic to. But what if you want to assign traffic to VLANs based on the source address and Ethernet protocol of the traffic? The latter is possible with MAC, IP, and protocol-based VLANs.

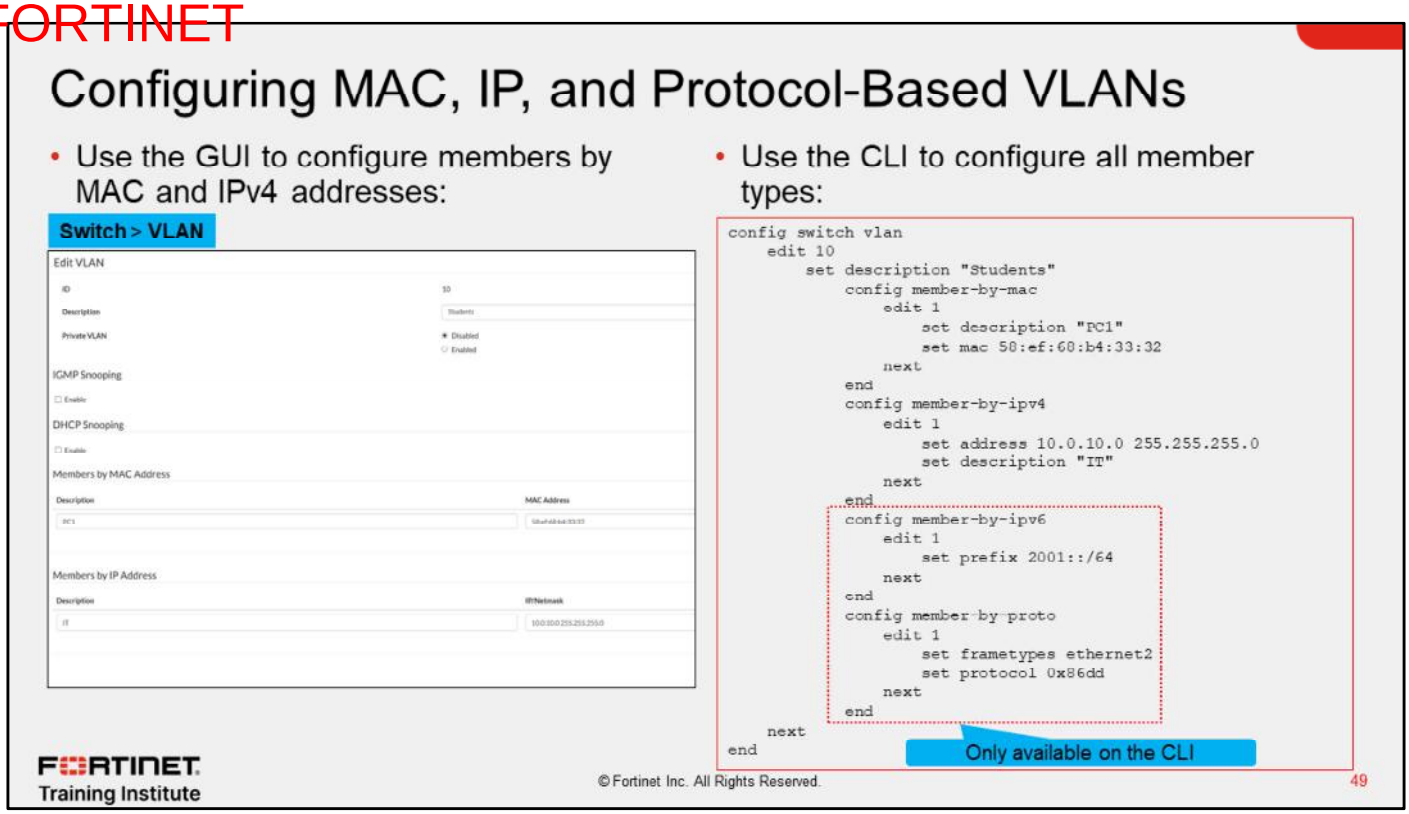
MAC, IP, and protocol-based VLANs enable you to assign ingress traffic to VLANs based on the endpoint source MAC address, source IP address, and Ethernet protocol (or Ethernet type). Then, when processing ingress traffic, FortiSwitch overrides the VLAN settings on the port with the VLAN assigned to the endpoint (or member) in the MAC, IP, and protocol-based VLAN configuration. One benefit is that you can place different devices behind the same switch port in different VLANs. Another benefit is mobility because endpoints can be assigned to the same VLAN regardless of the switch port they are connected to.

The benefits provided by MAC, IP, and protocol-based VLANs can also be obtained with 802.1X authentication. However, 802.1X is considered more scalable and secure, and therefore generally a better option. For this reason, MAC, IP, and protocol-based VLANs are more often used as a solution for specific scenarios rather than as the main VLAN assignment method in the network.

The example on this slide shows PC1 and PC2 behind port1 on FortiSwitch. The native VLAN on port1 is VLAN 20. Under standard VLAN operation, this would result in FortiSwitch tagging frames from PC1 with VLAN 20 when forwarding them to port2. However, because PC1 is a member of VLAN 10 (a member by MAC address), then FortiSwitch tags the frames from PC1 with VLAN 10 instead. Frames from PC2 that egress port2 are tagged with VLAN 20 because, unlike PC1, PC2 is not configured as a member of VLAN 10.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can configure VLAN members by MAC address and IPv4 address using the GUI, as shown on this slide. However, if you want to configure members by IPv6 address and Ethernet protocol, then you must use the CLI, as shown on this slide.

Note that the GUI screenshot has been cropped to fit on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

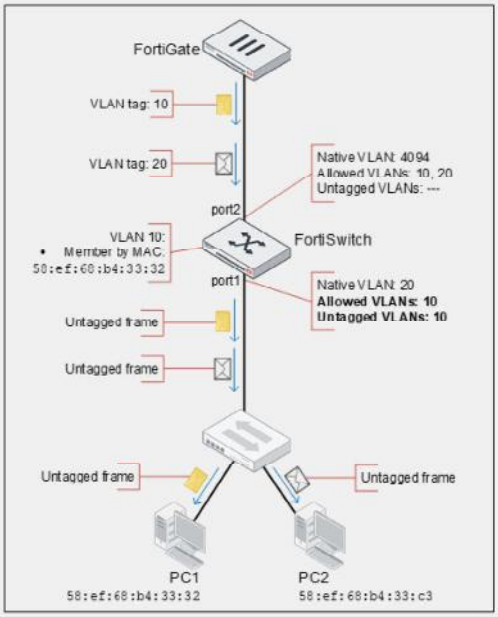
DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring MAC, IP, and Protocol-Based VLANs (Contd)

- Ensure VLAN settings on port allow traffic to endpoints:
  - Include VLAN ID that endpoint is member of in:
    - Allowed VLANs
    - Untagged VLANs *if* endpoint expects untagged traffic
- Set **Allowed VLANs** and **Untagged VLANs** on the GUI:

Switch > Interfaces





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

50

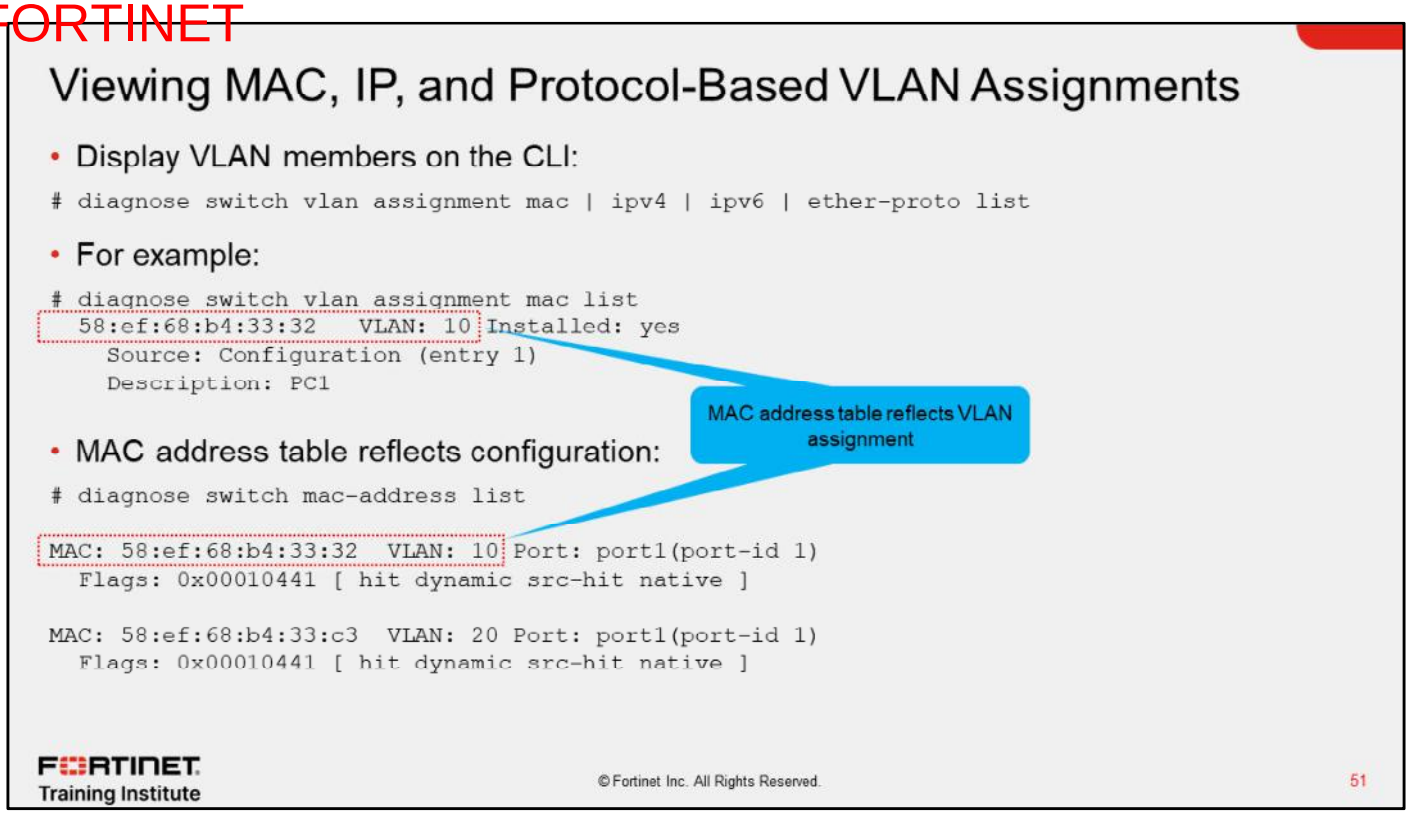
When MAC, IP, and protocol-based VLANs were introduced in this lesson, the example showed that the allowed VLANs and untagged VLANs settings on port1 were set to 10. These settings are required to allow the traffic destined to PC1.

The example on this slide shows the same topology as before, except that it is focused on the traffic destined to endpoints. When FortiSwitch receives on port2 frames destined to PC1, FortiSwitch won't forward the frames to port1 unless port1 is configured with VLAN 10 as the native VLAN, or if VLAN 10 is included in the allowed VLANs setting. If you are using MAC, IP, and protocol-based VLANs, then you probably don't want to change the native VLAN setting, which means that you must include VLAN 10 in the allowed VLANs setting. In addition, if the connected device expects to receive untagged traffic, then you must also include VLAN 10 in the untagged VLANs setting so FortiSwitch forwards the frames without a VLAN tag. For PC2, FortiSwitch can forward traffic to the device because VLAN 20 is set as the native VLAN on port1.

This slide also shows how you can configure the allowed VLANs and untagged VLANs settings using the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can review the assigned VLAN members by running the `diagnose switch vlan assignment` CLI command. This slide shows an example of the output displayed when querying the members by MAC.

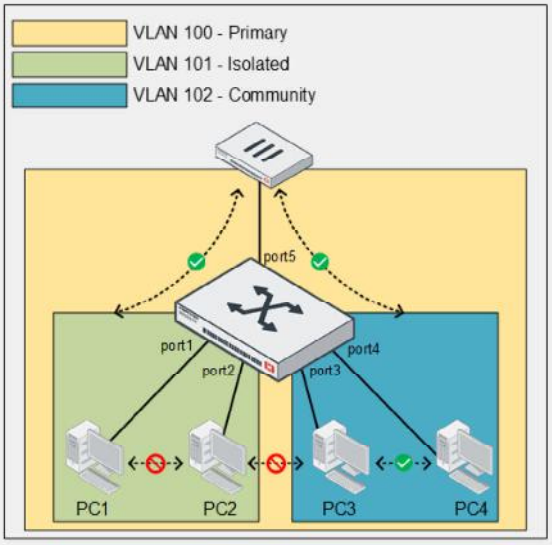
Note that the MAC address table also reflects the MAC, IP, and protocol-based VLAN assignments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

PVLANs

- Divides a primary VLAN into one or more secondary VLANs
  - Break down a VLAN broadcast domain
  - Further restrict access within a VLAN
- Two types of secondary VLANs
  - Isolated:
    - Allows communication with primary VLAN only
  - Community
    - Allows communication with primary VLAN and same community VLAN
- Port types:
  - P-Port:
    - Member of primary VLAN only (no secondary VLANs)
    - Usually for gateway devices (routers, firewalls)
  - I-Port:
    - Member of isolated VLAN
    - For devices requiring north-south traffic only
  - C-Port:
    - Member of community VLAN
    - For devices requiring north-south and limited east-west traffic



PVLAN Configuration			
Ports	Type	Primary VLAN	Secondary VLAN
port1, port2	I-Port	100	101
port3, port4	C-Port	100	102
port5	P-Port	100	---

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

52

A PVLAN divides a primary VLAN into one or more secondary VLANs. That is, a PVLAN divides a broadcast domain into multiple smaller broadcast subdomains. PVLANs enable you to further restrict access of devices in a VLAN without having to change their current IP addressing.

The are two types of secondary VLANs:

- Isolated: Hosts in this VLAN can communicate with hosts in the primary VLAN only. Communication with hosts in the same isolated VLAN, as well as communication with hosts in community VLANs is blocked.
- Community: Hosts in this VLAN can communicate with other hosts in the same community VLAN or with hosts in the primary VLAN. Communication with hosts in different secondary VLANs is blocked.

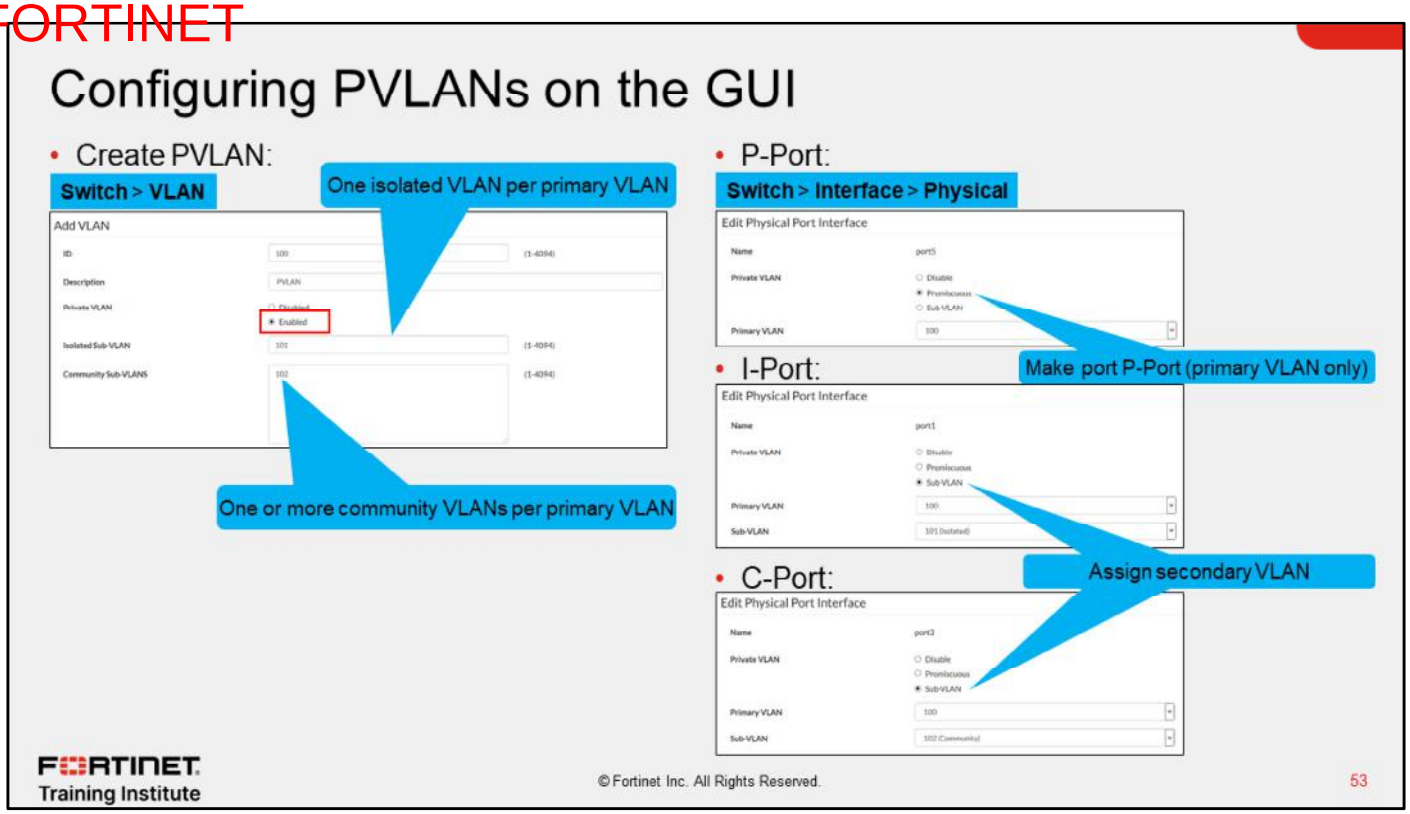
Depending on the PVLAN settings, a port is regarded as one of the following types:

- Promiscuous-Port (P-Port): A port that is a member of the primary VLAN only. No secondary VLANs are configured on this port. The host connected to this port can communicate with hosts in isolated VLANs or community VLANs. Usually, you want to configure this type of port on switch ports that connect to routers, firewalls, and other types of gateway devices.
- Isolated-Port (I-Port): A port that is a member of an isolated VLAN. A use case could be a server that needs to communicate with a gateway device only (north-south traffic), thus protecting the device from potential internal attacks.
- Community-Port (C-Port): A port that is a member of a community VLAN. A use case could be a server that needs to communicate with a gateway device, as well as with a few other devices in the same community VLAN for east-west traffic, thus restricting the communication to the minimum necessary.

The example on this slide shows how communication is restricted within a VLAN by using PVLANs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The first step to configure a PVLAN is to create the PVLAN on the **VLAN** page. Select **Enabled** to display the settings for secondary VLANs. Note that you can configure only one isolated VLAN per primary VLAN, but multiple community VLANs.

The next step is to configure the interface VLAN settings. In the example shown on this slide, port5, port1, and port3 are configured as P-Port, I-Port, and C-Port, respectively.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the group setting in ACLs used for?
   - A. It defines the user group to match in a packet.
   - ✓ B. It allows the same packet to match multiple ACL policies.

2. Which statement about MAC, IP, and protocol-based VLANs is true?
   - ✓ A. You may need to edit the allowed VLANs and untagged VLANs settings to allow traffic to the endpoint.
   - B. You can configure members by Ethernet protocol, on the GUI.

3. Which type of communication is allowed on devices in a community VLAN?
   - A. Communication with other devices in other community VLANs
   - ✓ B. Communication with devices in the primary VLAN

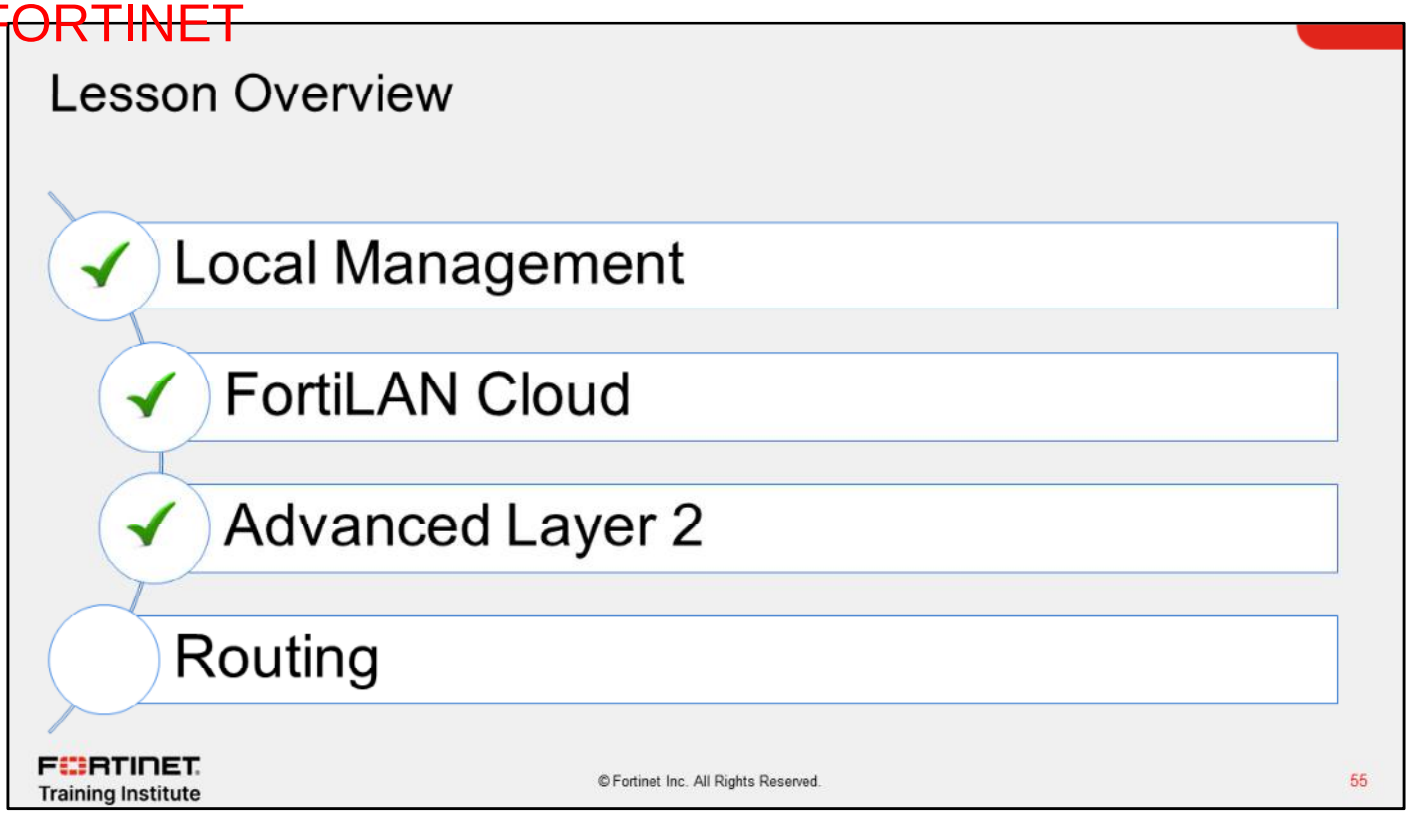
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

54

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

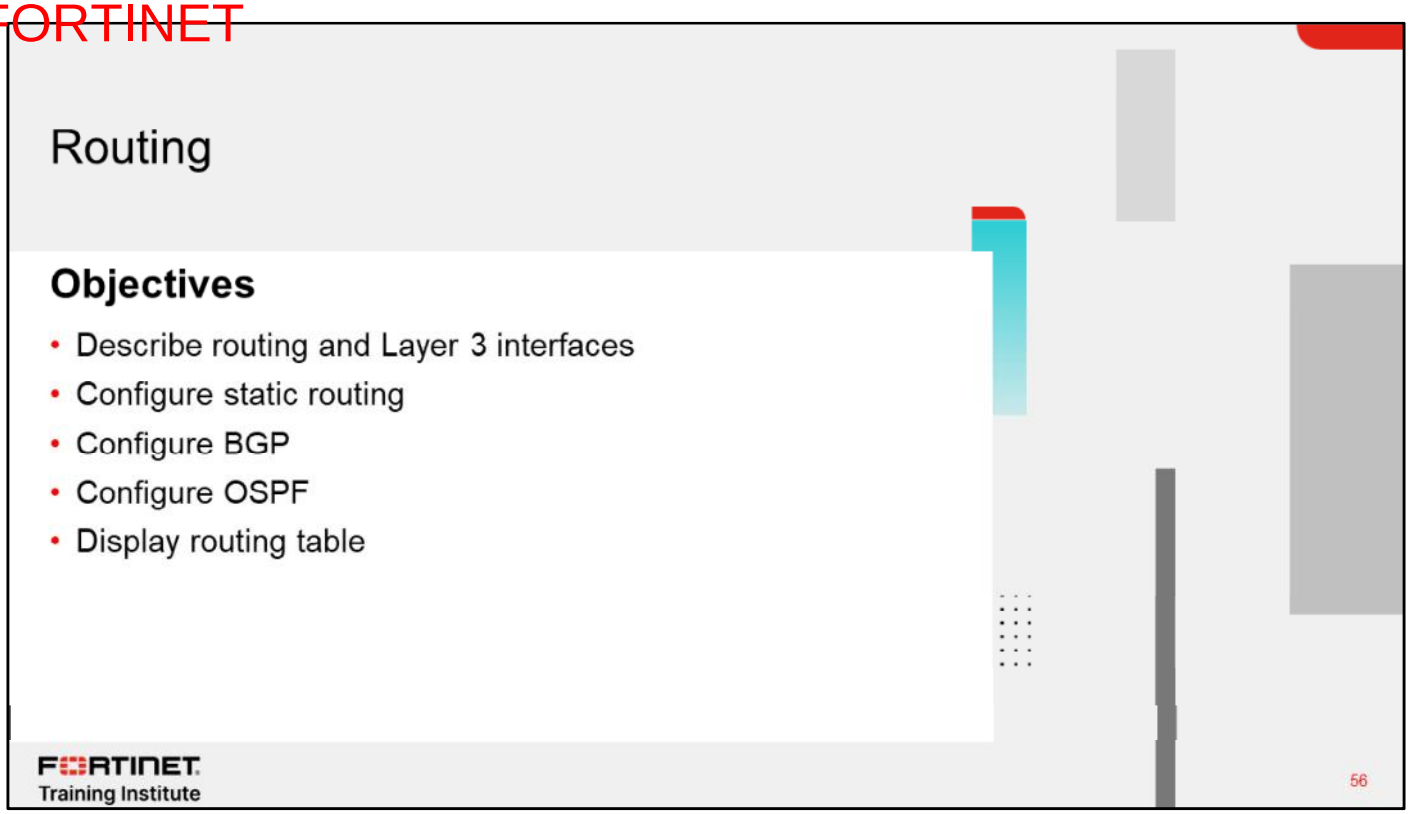


Good job! You now understand advanced Layer 2.

Now, you will learn about routing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

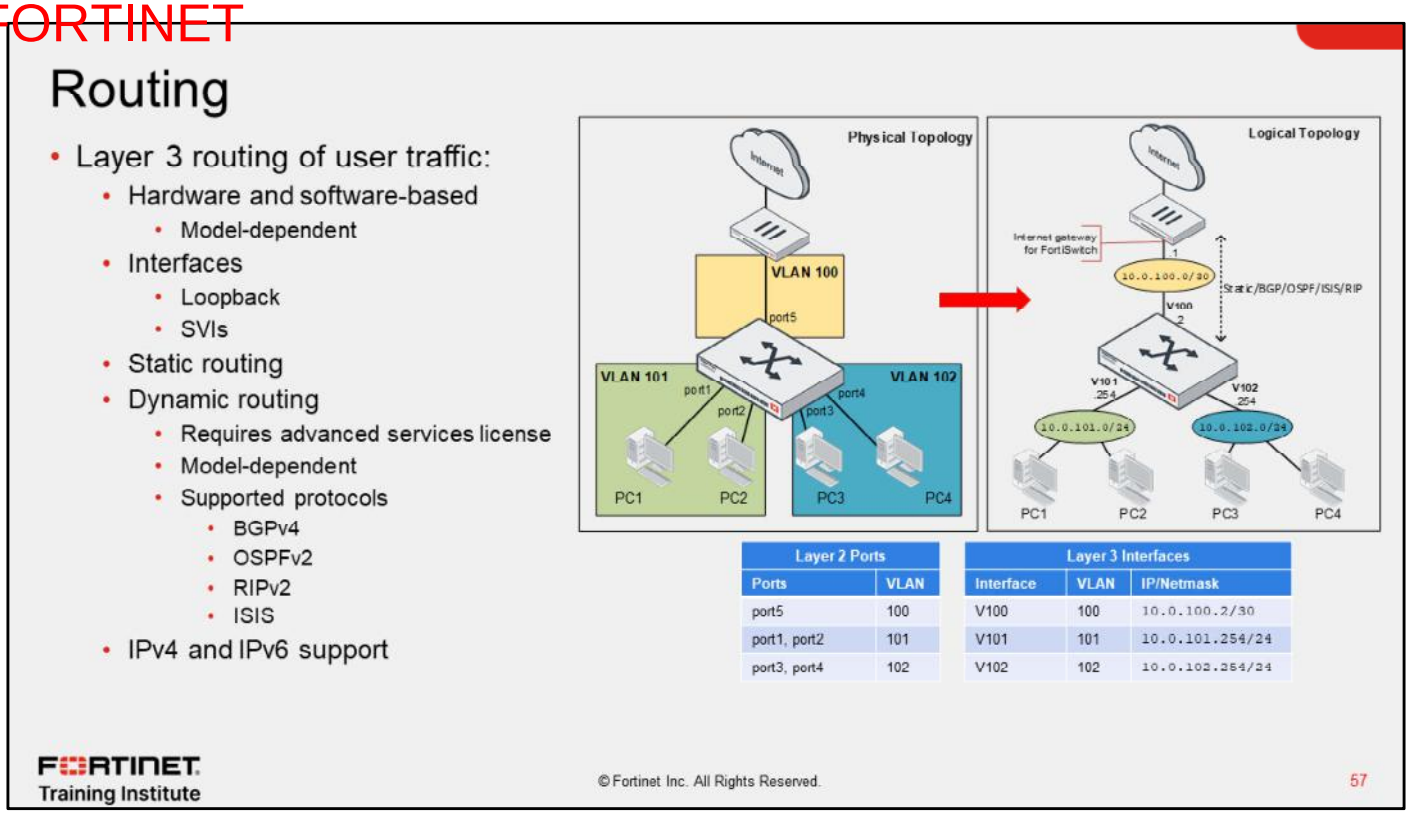


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in routing, you should be able to understand how to configure FortiSwitch to route user traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, FortiSwitch does Ethernet switching only. However, you can configure FortiSwitch to also route user traffic using static and dynamic routing. Note that dynamic routing requires an advanced services license.

Depending on the FortiSwitch model, routing is done on hardware or software. Hardware-based routing generally performs better because routing is done by ASIC, whereas software-based routing is done by the system CPU, which hinders performance.

You can configure Layer 3 interfaces to perform routing on FortiSwitch. The following types of Layer 3 interfaces are supported:

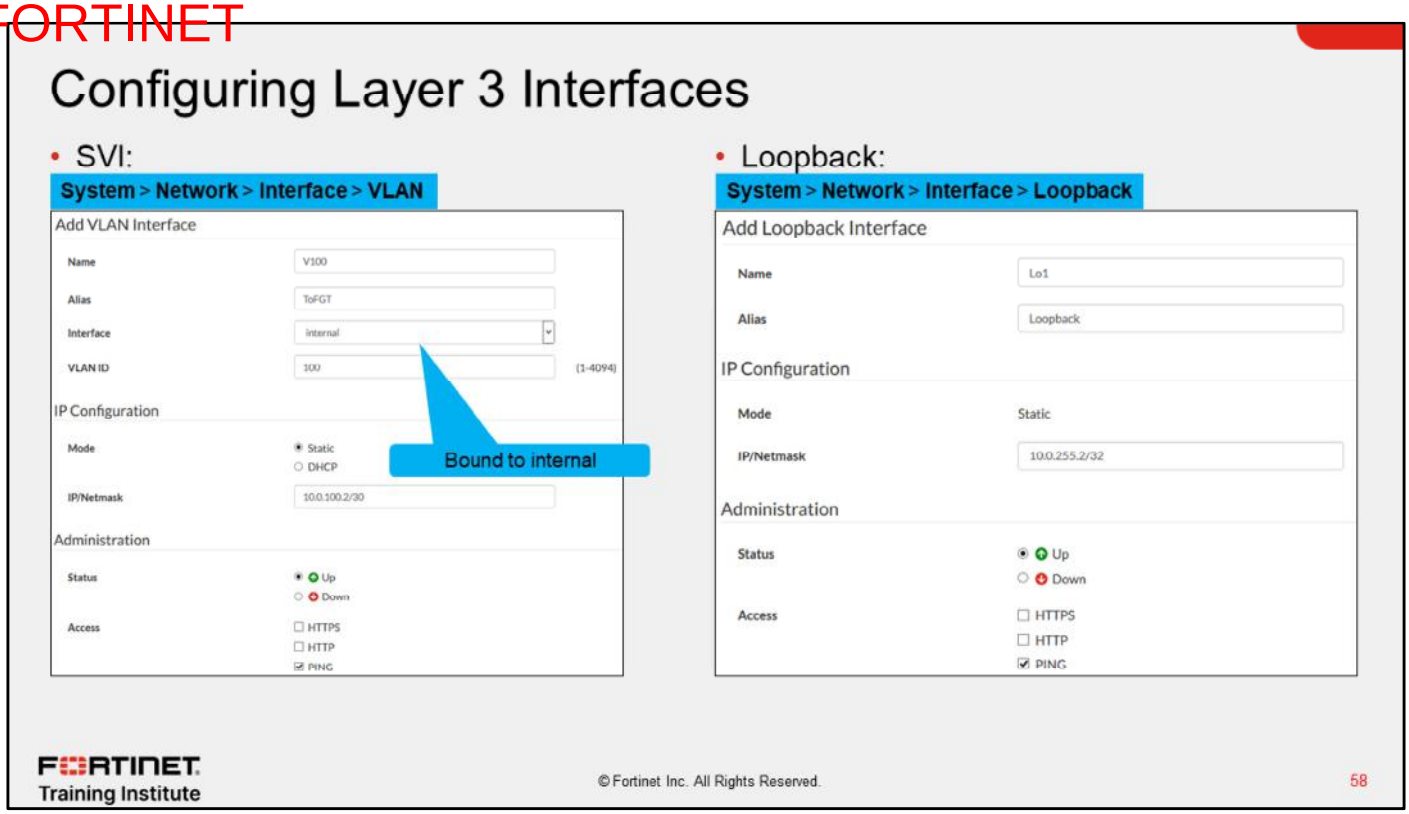
- Loopback: A logical interface that is not associated with any physical interface. It is commonly used as a reliable IP interface for dynamic protocol negotiation and updates.
- Switch virtual interface (SVI): A logical interface that is associated with a VLAN and that supports routing of user traffic. If you are familiar with FortiGate, think of an SVI as a VLAN interface.

All FortiSwitch models that support routing can perform static routing. However, depending on the model, some or all of the following dynamic routing protocols are supported: BGPv4, OSPFv2, RIPv2 and ISIS. Refer to the FortiSwitch datasheet at `fortinet.com` to know which models perform hardware or software-based routing, which models support dynamic routing, and the dynamic routing protocols they support.

The example on this slide shows FortiSwitch as a Layer 3 router. FortiSwitch performs inter-VLAN routing between endpoints. FortiSwitch also forwards internet traffic to FortiGate, which acts as the internet gateway. FortiSwitch is configured with three SVIs: V100, V101, and V102. V100 acts as the IP interface to route traffic to and from FortiGate. This could be done using static or dynamic routing. V101 and V102 act as the LAN gateway for endpoints in VLANs 101 and 102, respectively.

Vouchers & Dumps are Available | WhatsApp +201224560923

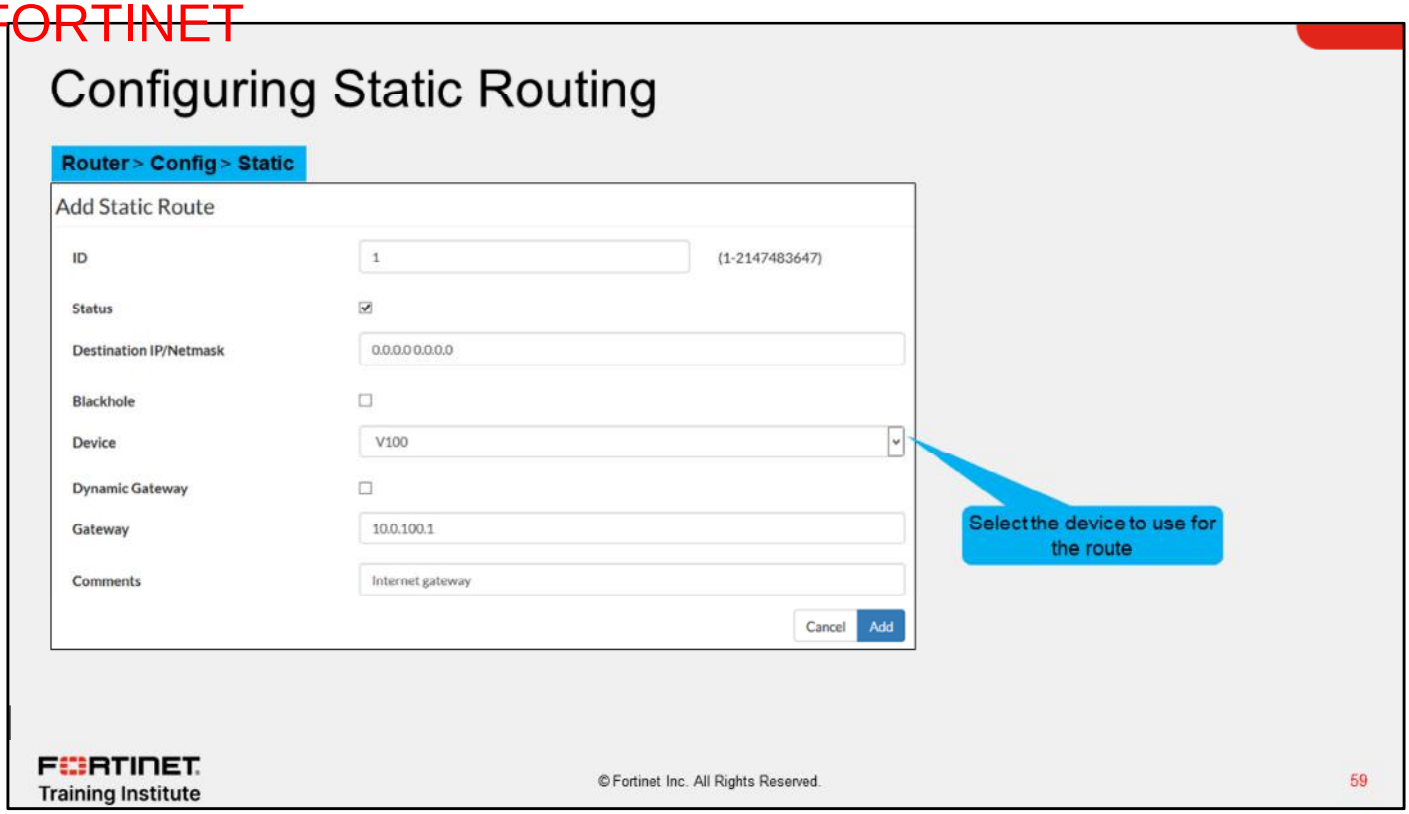
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows how to configure an SVI and a loopback interface on the GUI. Note that you must bind an SVI to the internal interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

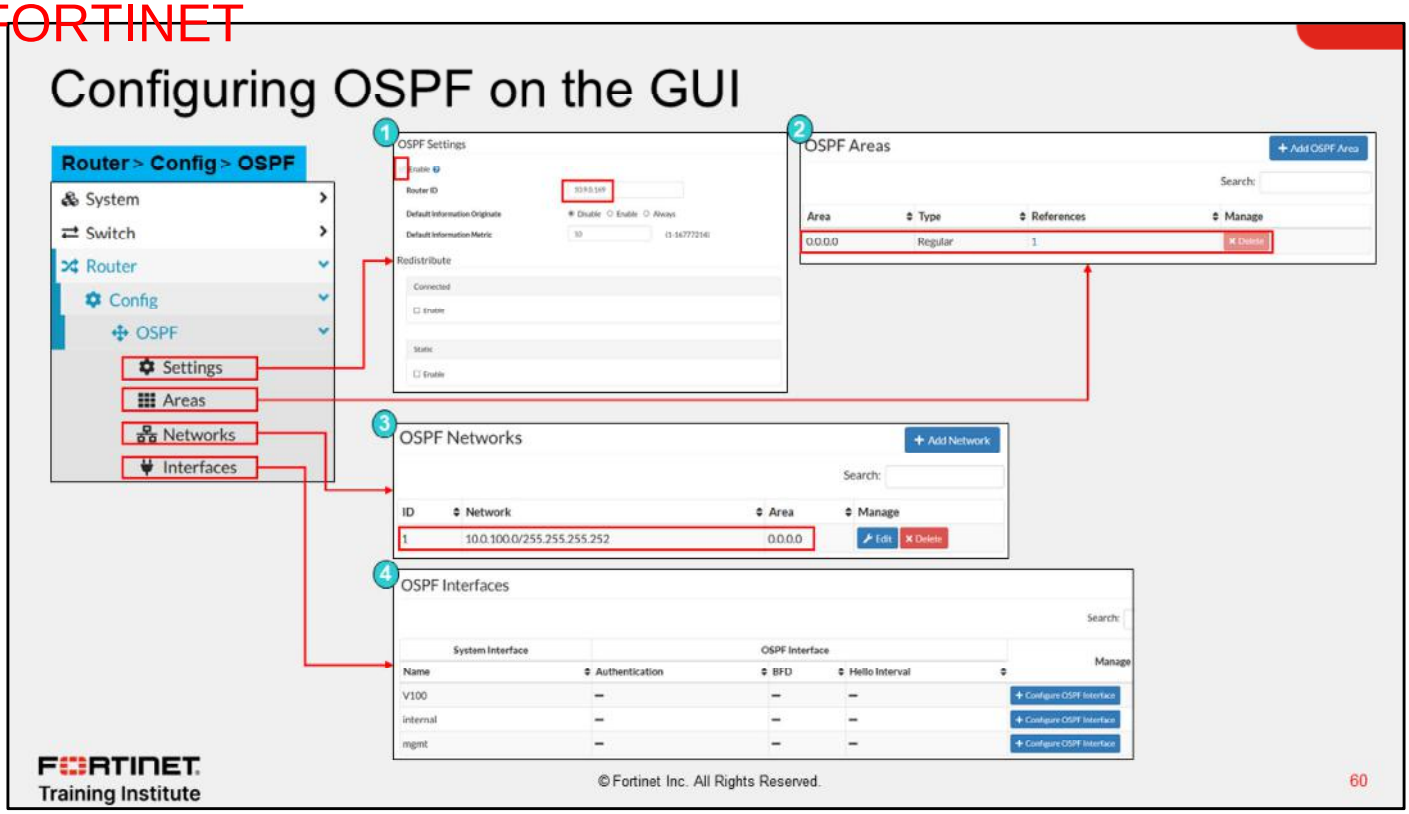
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows a default static route configured on the GUI. Note that you must select the interface (or device) that the route uses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If your FortiSwitch has a valid advanced services license, the FortiSwitch GUI shows an **OSPF** submenu that you can use to configure OSPF. The example on this slide shows a basic OSPF configuration on each of the four OSPF sections available on the GUI. The four sections are described next:

- **OSPF Settings**: This is your starting point in the OSPF configuration. Here, you enable OSPF, set the OSPF router ID, and optionally select which route types to redistribute into OSPF. The example on this slide shows `10.9.0.169` as the OSPF router ID, and no redistributed routes.

- **OSPF Areas**: After you enable OSPF, you must configure in this section at least one OSPF area that OSPF participates in. The example on this slide shows a configuration for the backbone area (area `0.0.0.0`).

- **OSPF Networks**: This is where you configure one or more OSPF networks in an OSPF area. The networks determine the Layer 3 interfaces FortiSwitch turns OSPF on. The example on this slide shows the network `10.0.100.0/30` configured in the backbone area.

- **OSPF Interfaces**: Optionally, you can edit the default OSPF settings on the system interfaces (or Layer 3 interfaces). The system interfaces include **mgmt**, **internal**, and SVIs. You can configure interface settings such as the OSPF timers, MTU, cost, authentication, and so on. The example on this slide shows the system interfaces with default settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring OSPF on the CLI

```
config router ospf
    set router-id 10.9.0.169
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set area 0.0.0.0
                set prefix 10.0.100.0 255.255.255.252
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "bgp"
        end
        config redistribute "rip"
        end
        config redistribute "isis"
        end
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

61

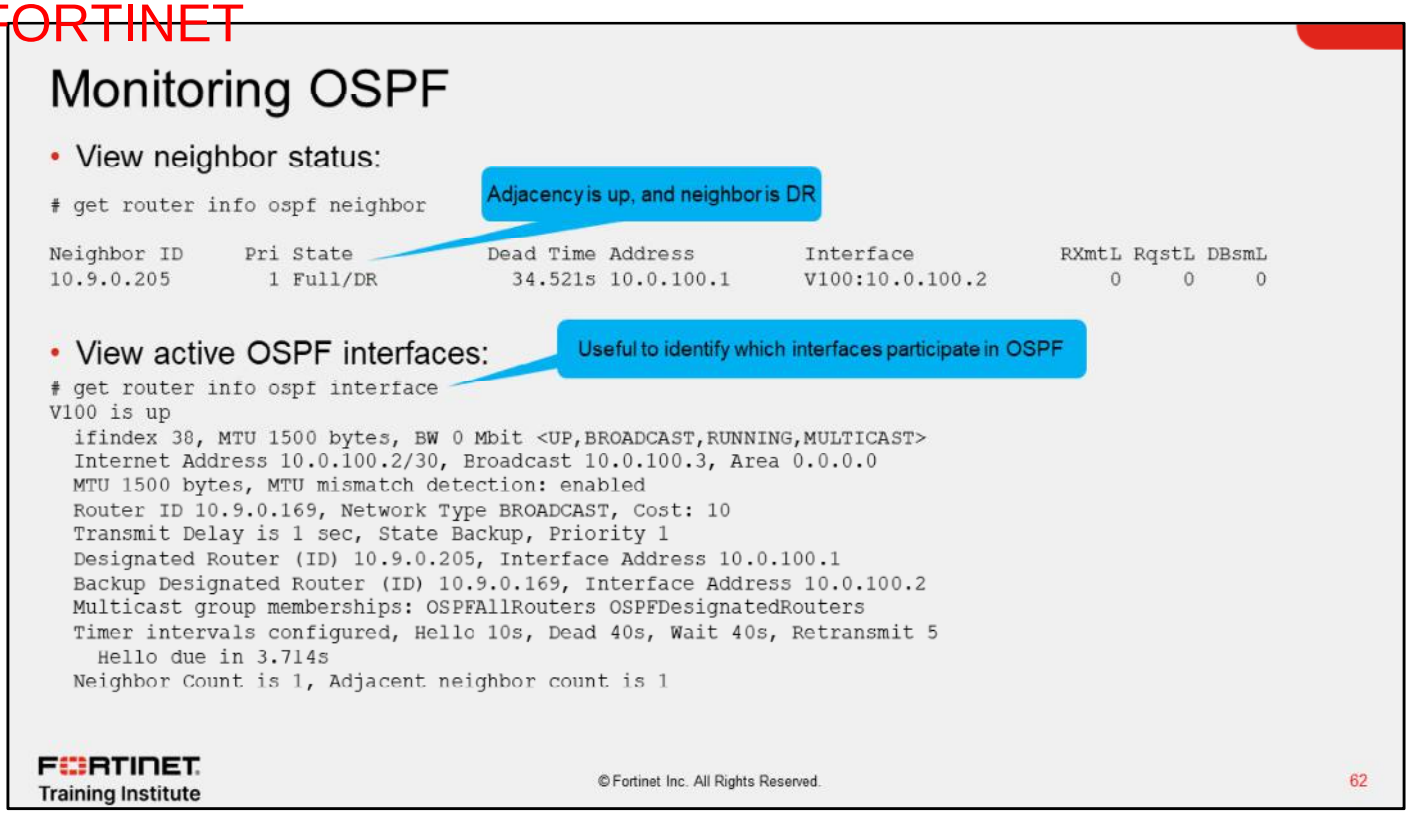
Alternatively, you can configure OSPF using the FortiSwitch CLI. The CLI provides you with many more settings to configure OSPF. Usually, advanced OSPF users start off by configuring basic OSPF settings on the FortiSwitch GUI, and then continue the setup on the CLI to configure advanced settings.

The example on this slide shows the equivalent CLI configuration applied previously on the GUI. Like the GUI, the CLI shows an OSPF configuration node only if FortiSwitch has a valid advanced services license. If you are familiar with OSPF configuration in FortiOS, notice that the OSPF configuration in the FortiSwitchOS CLI is very similar to FortiOS.

Refer to the *FortiSwitchOS CLI Reference* guide at `docs.fortinet.com` to get the full list of settings available for OSPF on the CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



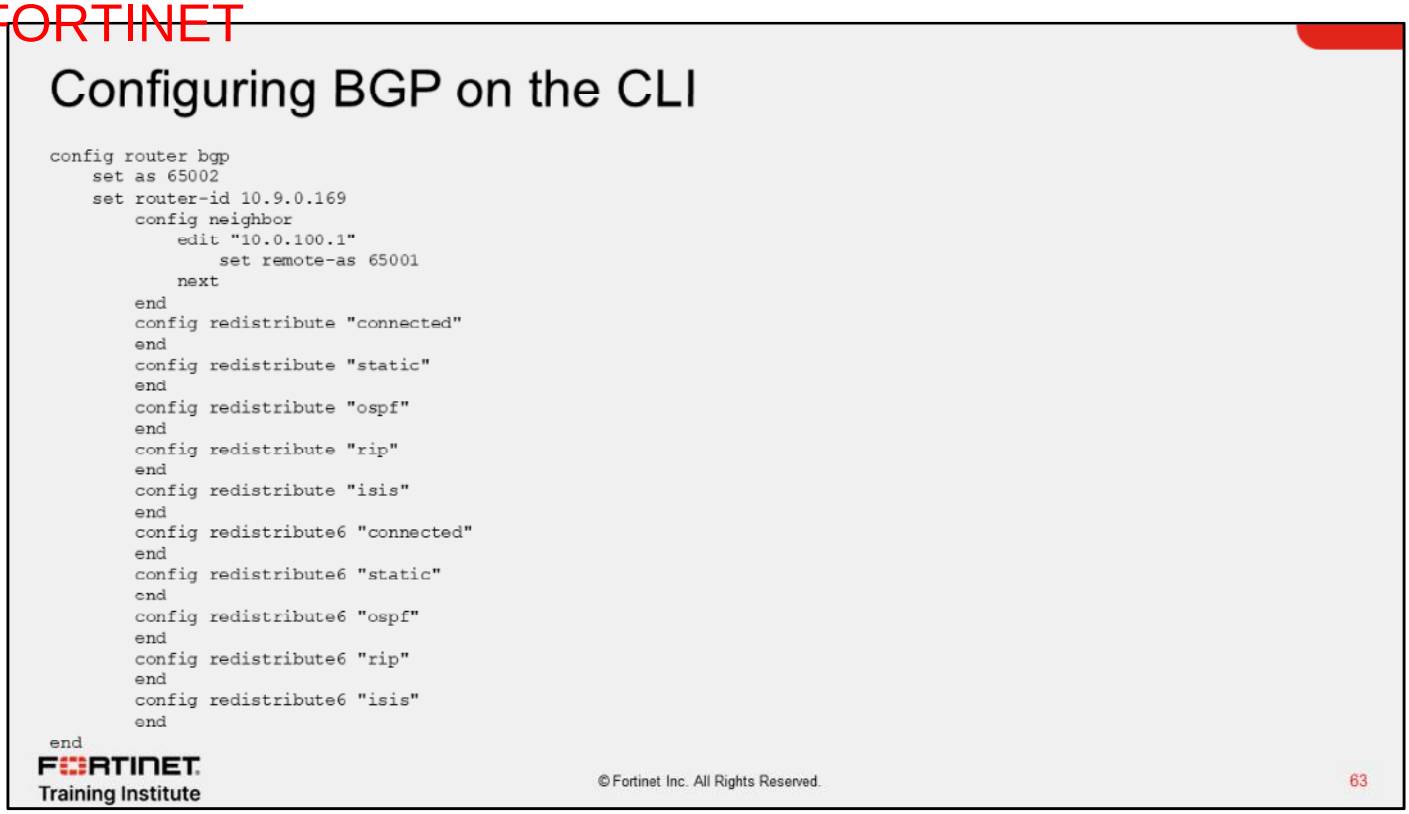
This slide shows two of the most common OSPF monitoring CLI commands. You can use the `get router info ospf neighbor` command to get the status of OSPF adjacencies on FortiSwitch. The example on this slide shows that the adjacency with neighbor ID `10.9.0.205` is up (full synchronization), and that the neighbor is the designated router (`DR`).

Another useful CLI command is `get router info ospf interface`. You can use this command to get the list of the system interfaces that participate in OSPF. In the example shown on this slide, `V100` is the only interface participating in OSPF.

Refer to the *FortiSwitchOS CLI Reference* guide at `docs.fortinet.com` to get the full list of monitoring commands available for OSPF.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can configure BGP on the FortiSwitch CLI only. In addition, BGP is supported on high-end FortiSwitch models only, provided the switch has a valid advanced services license.

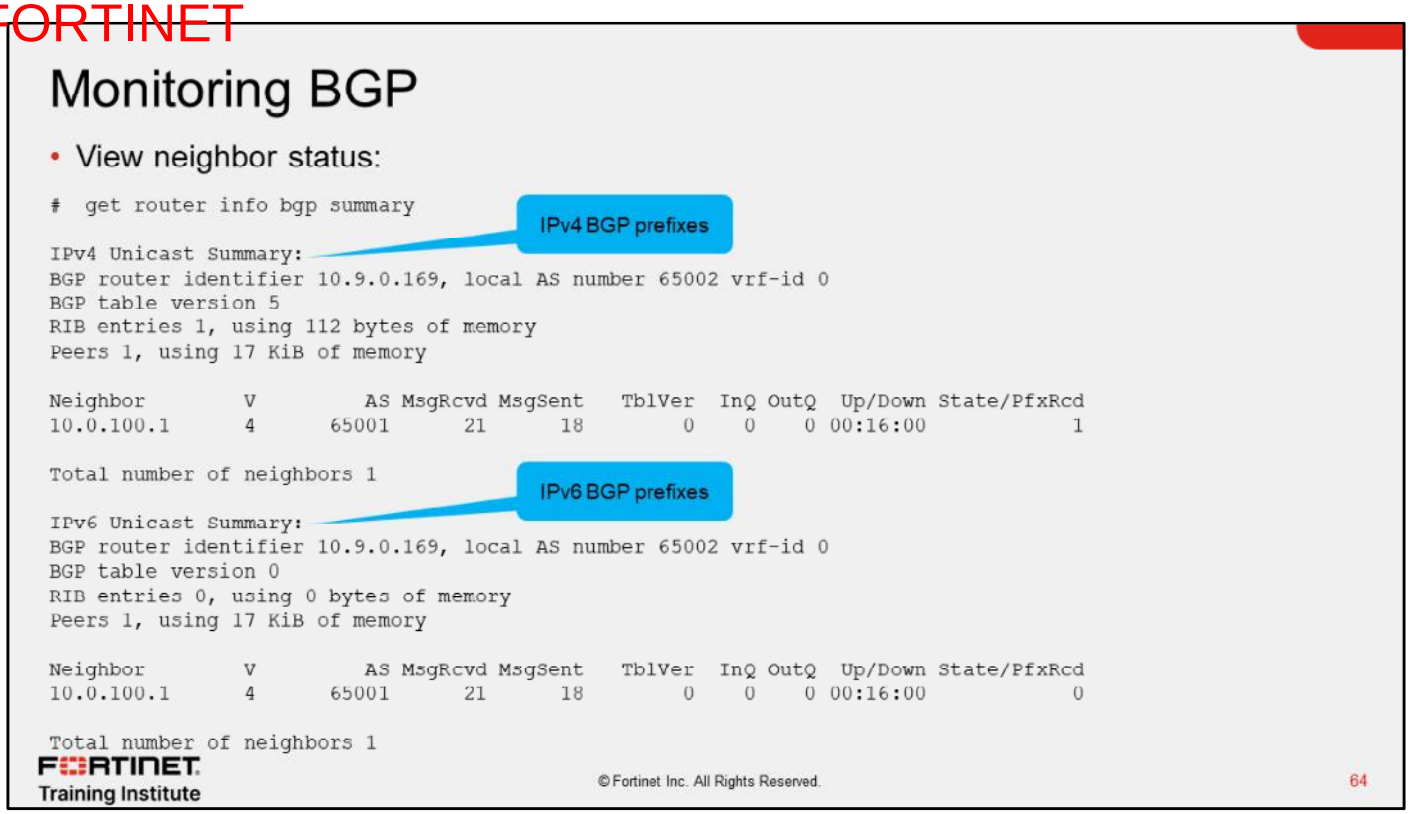
The example on this slide shows a very basic BGP configuration. FortiSwitch is assigned `65002` and `10.9.0.169` as the autonomous system (AS) and BGP router ID, respectively. In addition, FortiSwitch is configured to peer with the external BGP neighbor `10.0.100.1`, which uses `65001` as its AS.

If you are familiar with BGP configuration in FortiOS, notice that the BGP configuration in the FortiSwitchOS CLI is very similar to FortiOS.

Refer to the *FortiSwitchOS CLI Reference* guide at `docs.fortinet.com` to get the full list of settings available for BGP on the CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



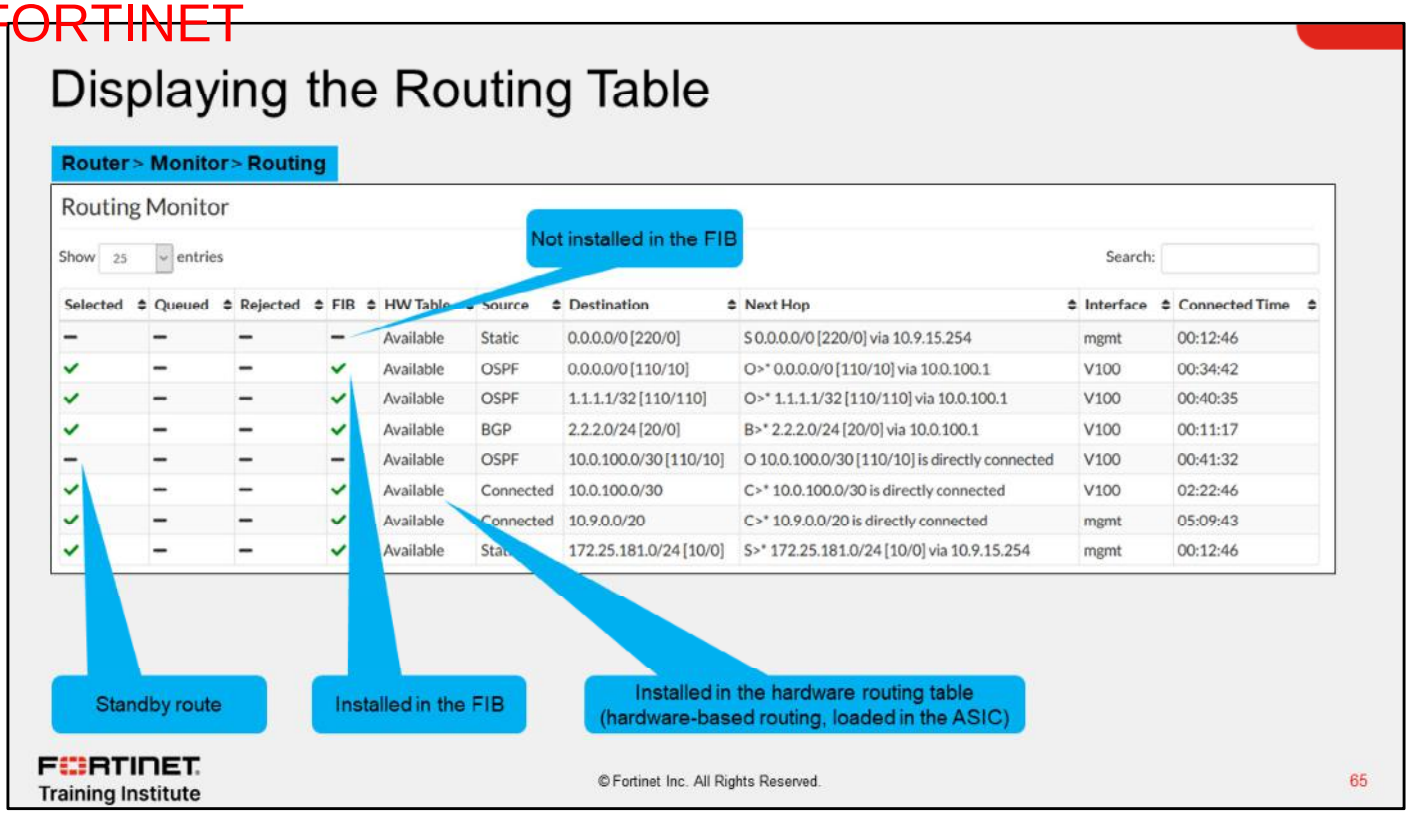
This slide shows an example of the output produced by the `get router info bgp summary` CLI command. The command is commonly used for monitoring BGP on FortiSwitch, and displays the status of all BGP peerings. The example on this slide shows that the peering with neighbor `10.0.100.1` is up, and that FortiSwitch received one prefix from that neighbor.

Note that the output contains two sections: one for IPv4 and another for IPv6. Each section indicates the number of IPv4 or IPv6 prefixes received. The example on this slide shows that no IPv6 prefixes were received from neighbor `10.0.100.1`.

Refer to the *FortiSwitchOS CLI Reference* guide at `docs.fortinet.com` to get the full list of monitoring commands available for BGP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



At first glance, the FortiSwitch routing table displays the same standard information found in other routing tables. One difference, however, is the presence of the **Selected**, **Queued**, **Rejected**, **HW Table**, and **FIB** columns, which are explained next:

- **Selected**: indicates whether the route is the best route for the destination network.
- **Queued**: indicates whether the route is waiting to be installed in the hardware routing table. Routes are first queued before being installed in the hardware routing table. This process usually happens very fast.
- **Rejected**: indicates routes that are not supported and therefore, are rejected by FortiSwitch.
- **FIB**: indicates routes that are installed in the forwarding information base (FIB). Like FortiGate, FortiSwitch maintains a FIB, which is composed of the *best* (or *selected*) connected, static and dynamic routes. Note the use of *best*. This is because, like FortiGate, not all routes are installed in the FortiSwitch FIB. Only the best routes per destination network are.
- **HW Table**: indicates which routes in the FIB are installed in the hardware routing table. FortiSwitch looks up the hardware routing table first and, if there is no match, tries the FIB. Hardware-based routing is done when FortiSwitch uses routes in the hardware routing table, which are loaded in the ASIC. Software-based routing is done when FortiSwitch uses the routes in the FIB, which are loaded in the kernel.

In the example shown on this slide, the first route in the table, which is a static default route with a distance of `220`, is not installed in the FIB because FortiSwitch preferred the default route learned through OSPF, which has a lower distance (`110`). The static route, however, remains on standby and is installed in the FIB if the OSPF route is removed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about dynamic routing is true?
   - ✓ A. It requires a valid advanced services license.
   - B. It is supported on all FortiSwitch models.

2. Which statement about hardware-based routing is true?
   - A. When hardware-based routing is used, routes are loaded in the kernel.
   - ✓ B. Hardware-based routing usually performs better than software-based routing.

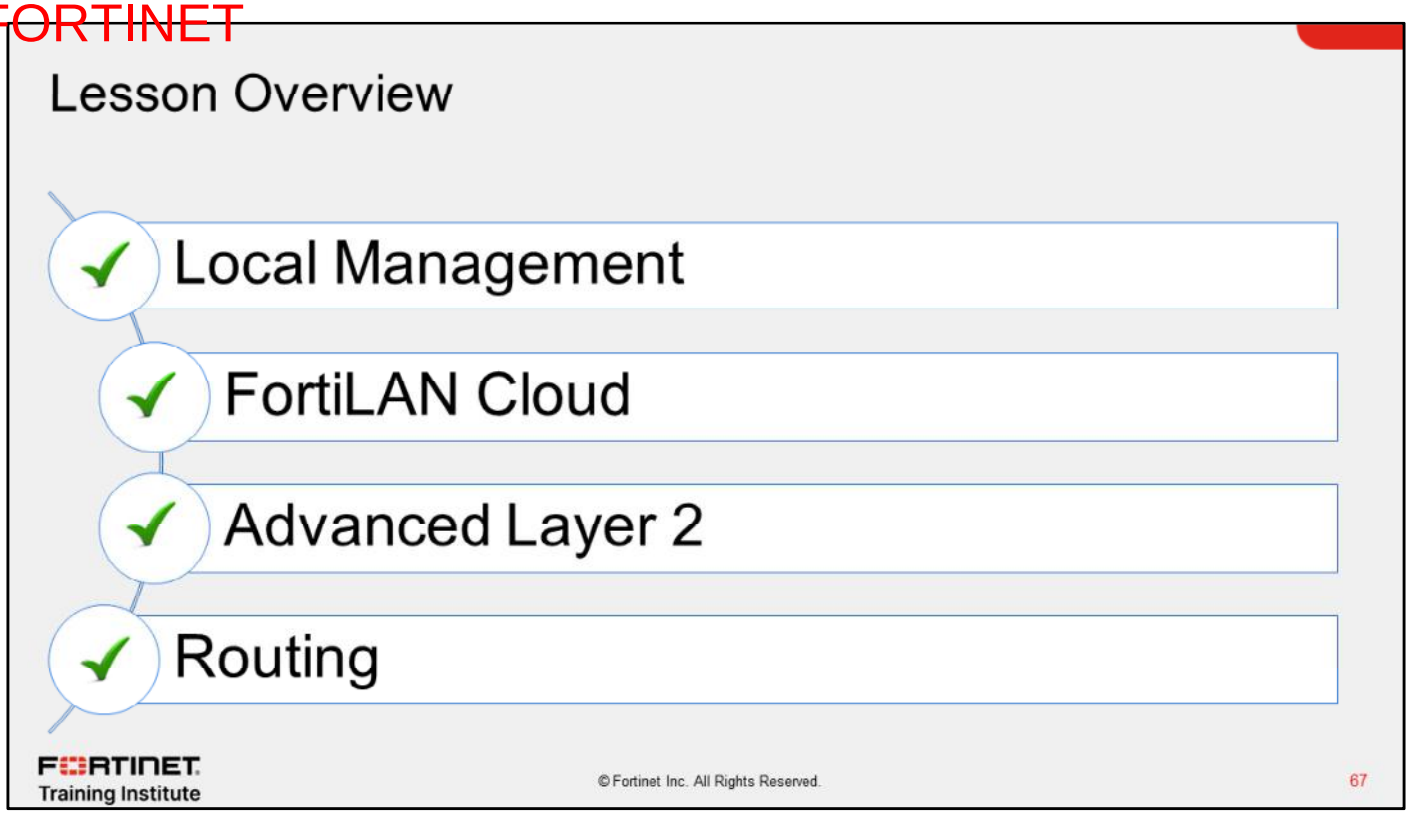
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

66

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

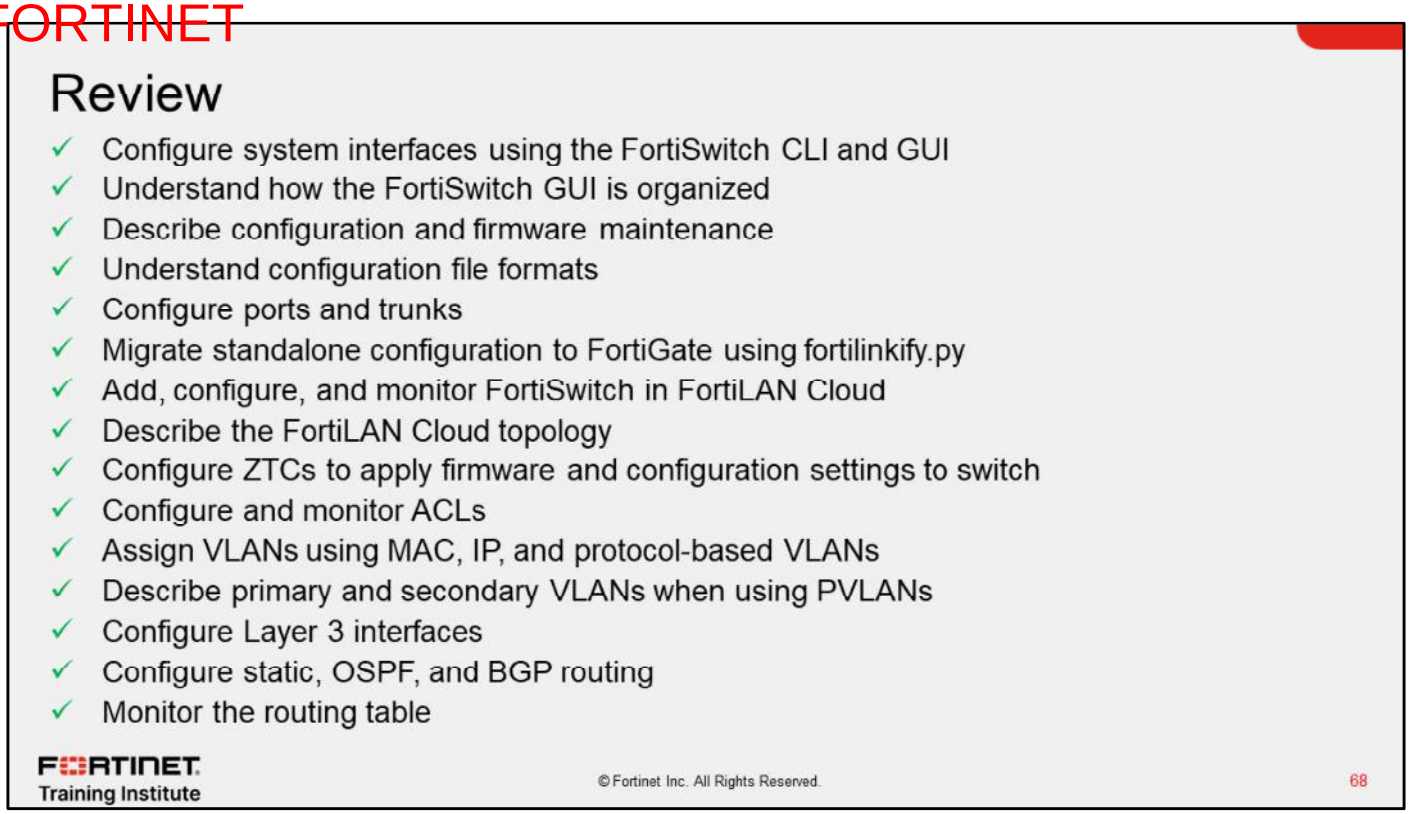


Good job! You now understand routing.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

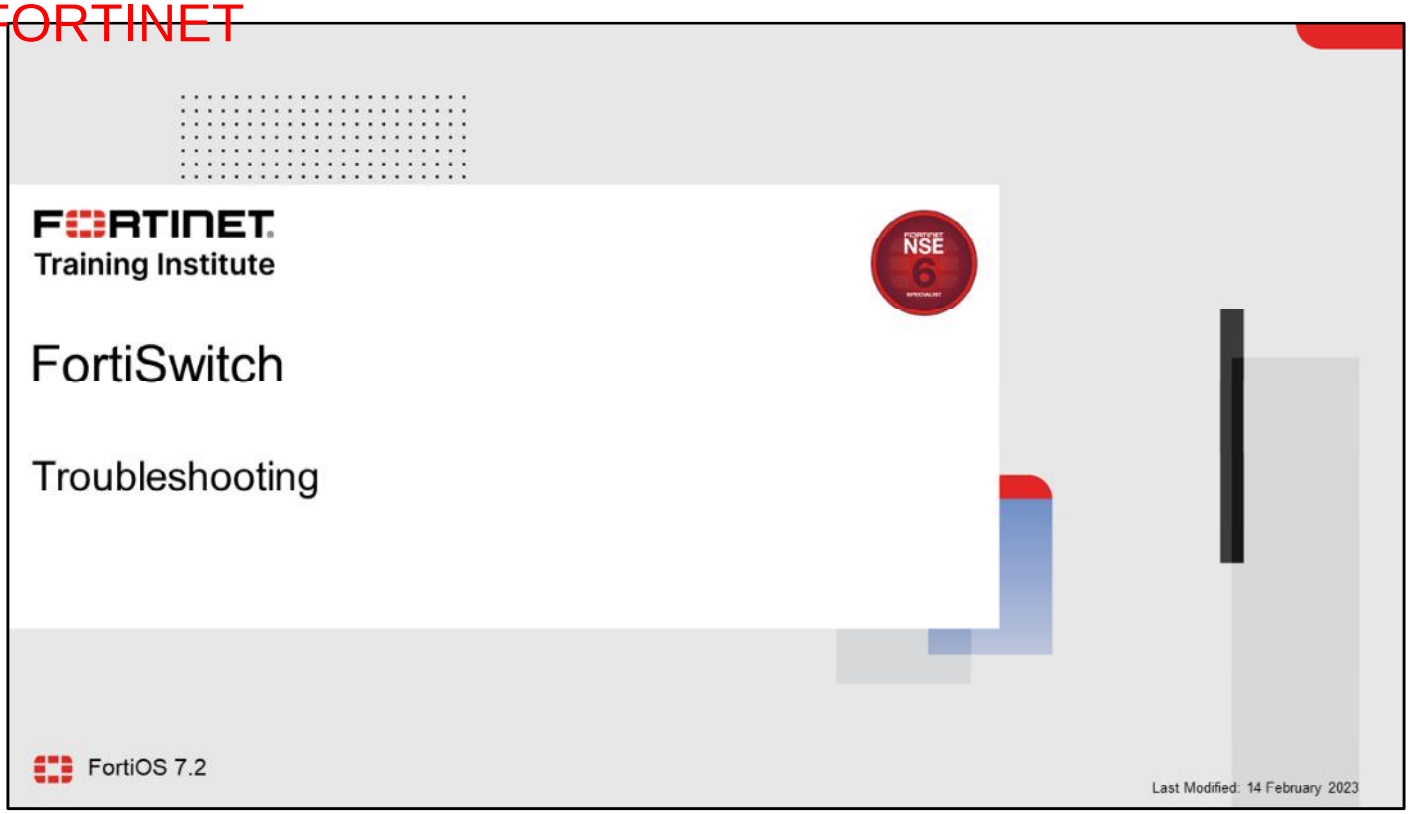


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned which features are available on FortiSwitch when it is running in standalone mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

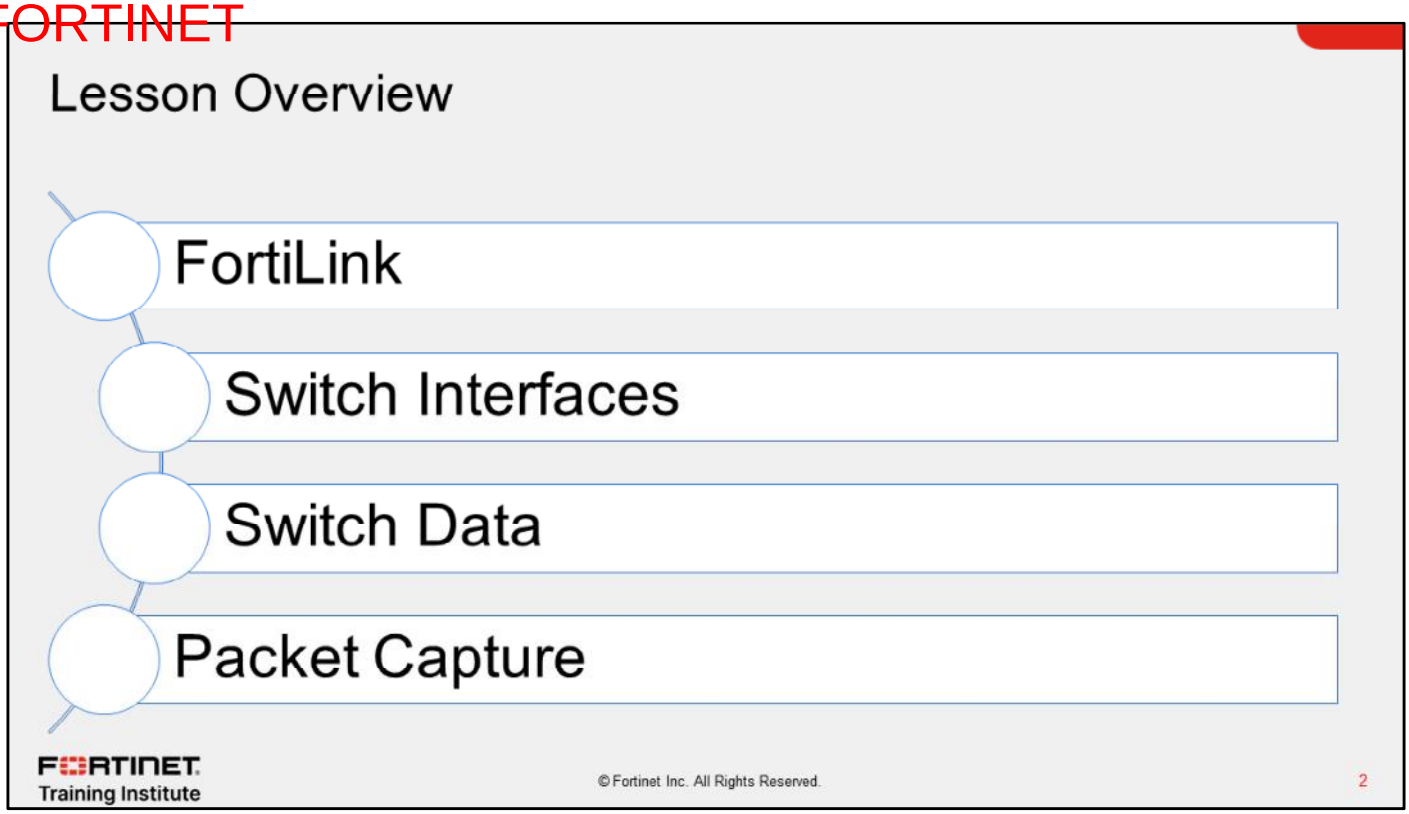
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the most useful tools at your disposal to troubleshoot FortiSwitch-related issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

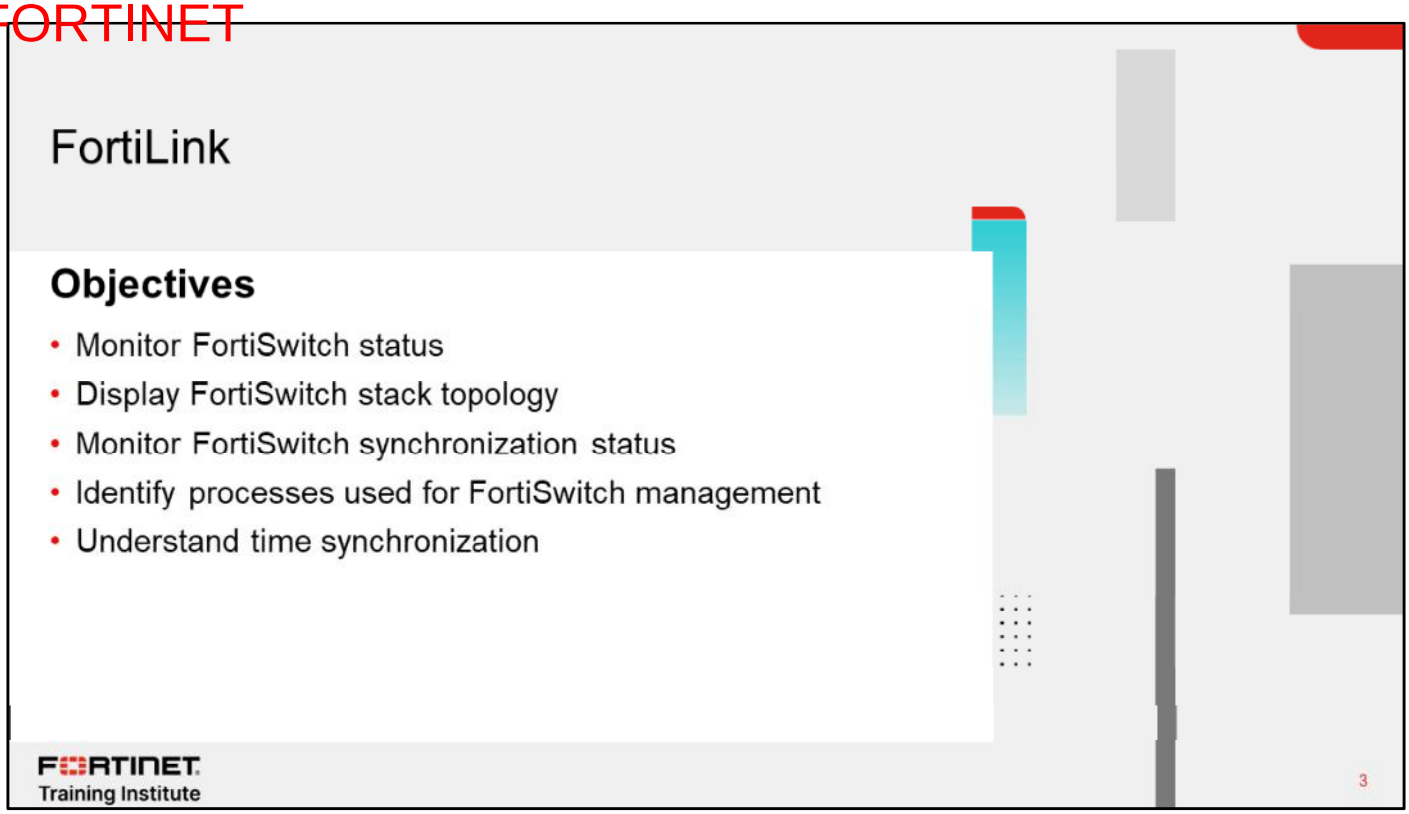
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

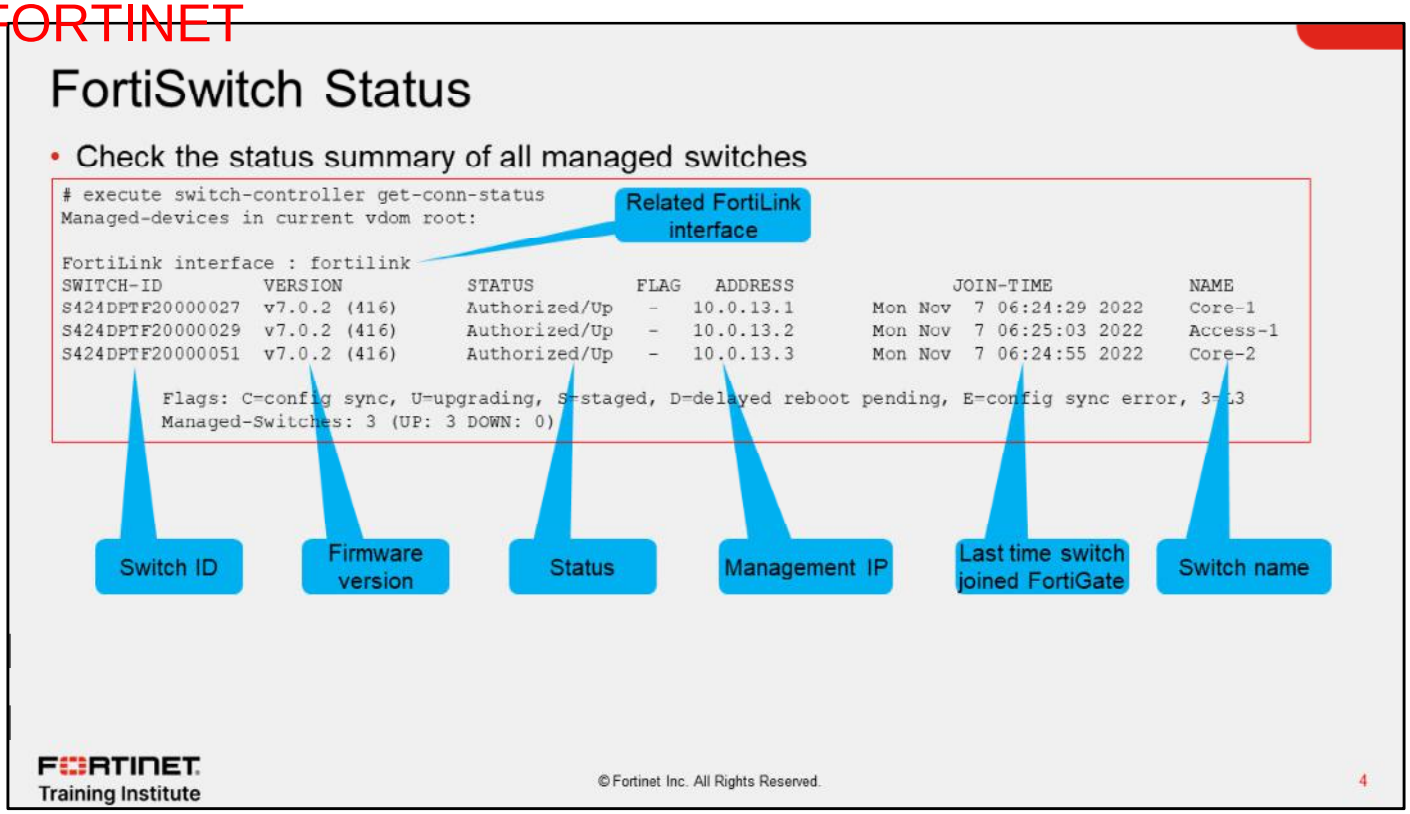


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiLink troubleshooting, you should be able to understand how to troubleshoot management issues when FortiSwitch is managed by FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

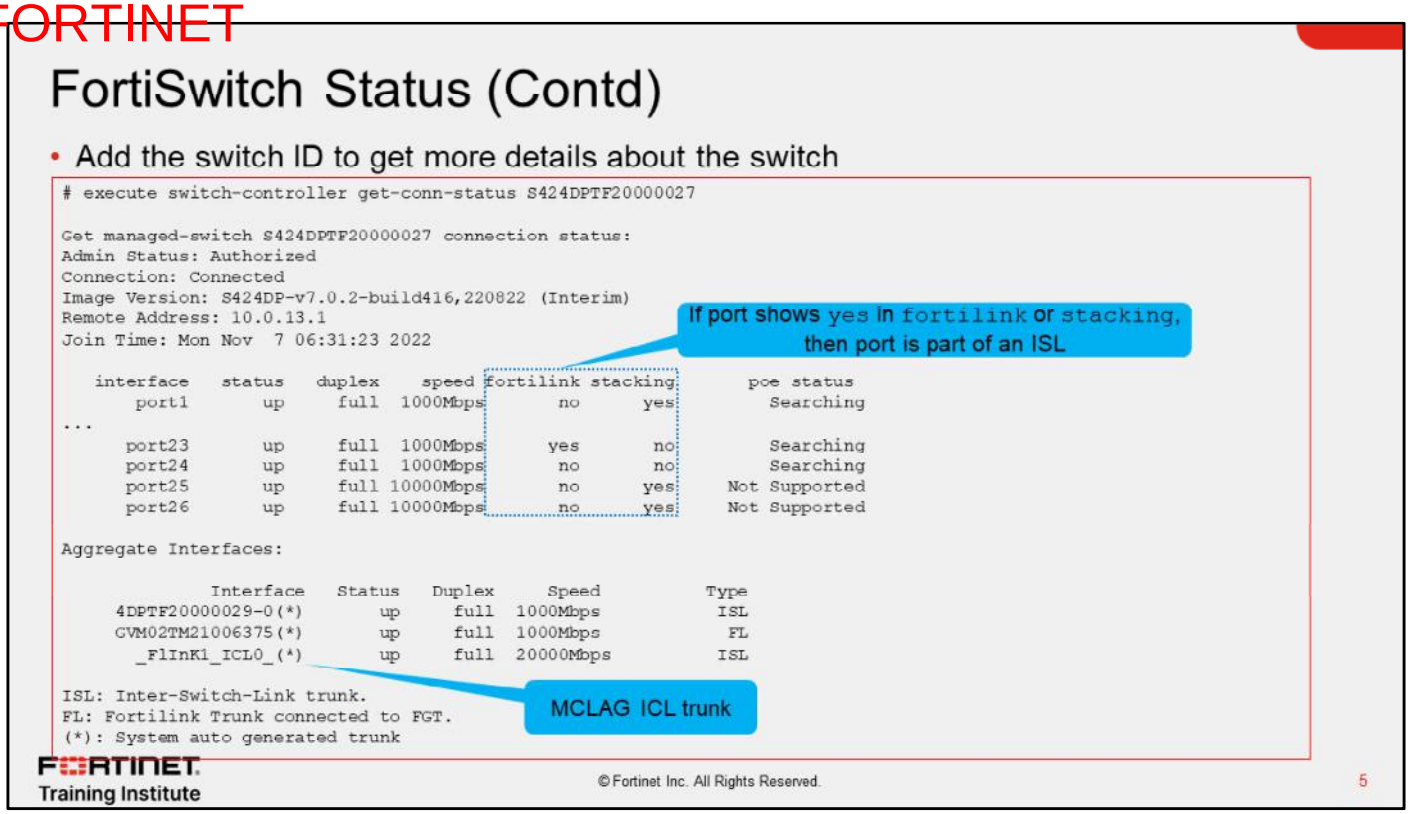


When troubleshooting managed switches, you probably want to start by running `execute switch-controller get-conn-status` on the FortiGate CLI. The command provides you with key information for all managed switches, such as their current status, management IP address, firmware version, as well as the last time the switches successfully connected to (or joined) FortiGate. Under normal operation, a switch join time should remain the same. However, if a switch join time is frequently getting updated, this may be an indication of connectivity issues between the switch and FortiGate.

The output also provides you with two pieces of information that you will likely need to troubleshoot further: the name of the FortiLink interface the stack is connected to and the ID of the switches in the stack. Because FortiGate supports management of multiple switch stacks, and given that each stack can have multiple switches, knowing the FortiLink interface that the stack is connected to and the switch ID of a problematic switch will enable you to filter the output obtained when running troubleshooting commands. This is particularly useful when dealing with large FortiSwitch deployments because going over the output of all managed switches can be overwhelming. In the example shown on this slide, the FortiLink interface is `fortilink`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

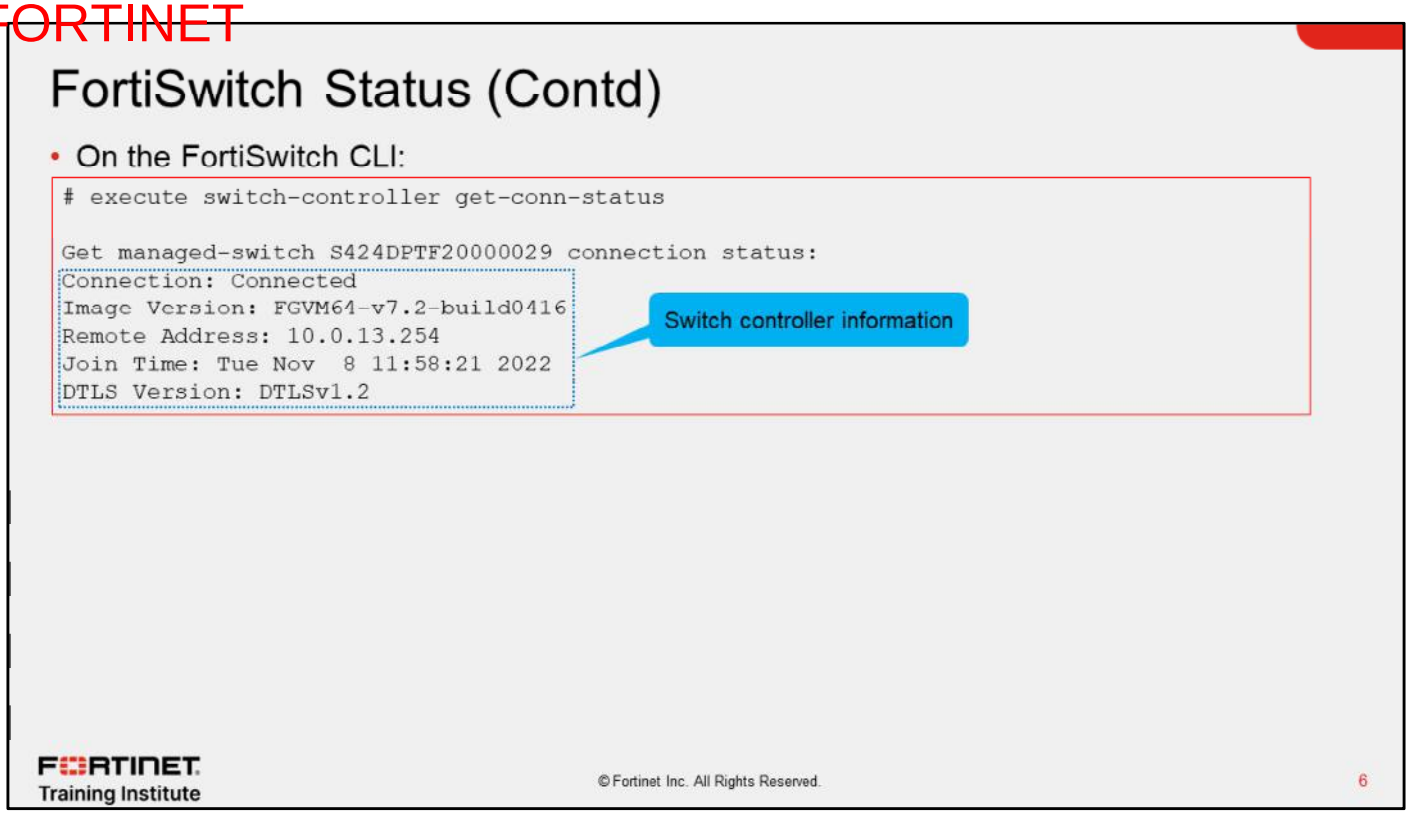


If you add the switch ID to the `execute switch-controller get-conn-status` command, you get further details about the switch, including the status summary of all of its ports and aggregate interfaces (or trunks). The `fortilink` and `stacking` columns indicate whether the port is part of an ISL.

In the `Aggregate Interfaces` section, the `ISL` and `FL` flags shown in the example on this slide indicate that there is one FortiLink trunk, and two ISLs. The name of the last ISL in the list suggests that the trunk is used as a multi-chassis link aggregation (MCLAG) ICL.

Vouchers & Dumps are Available | WhatsApp +201224560923

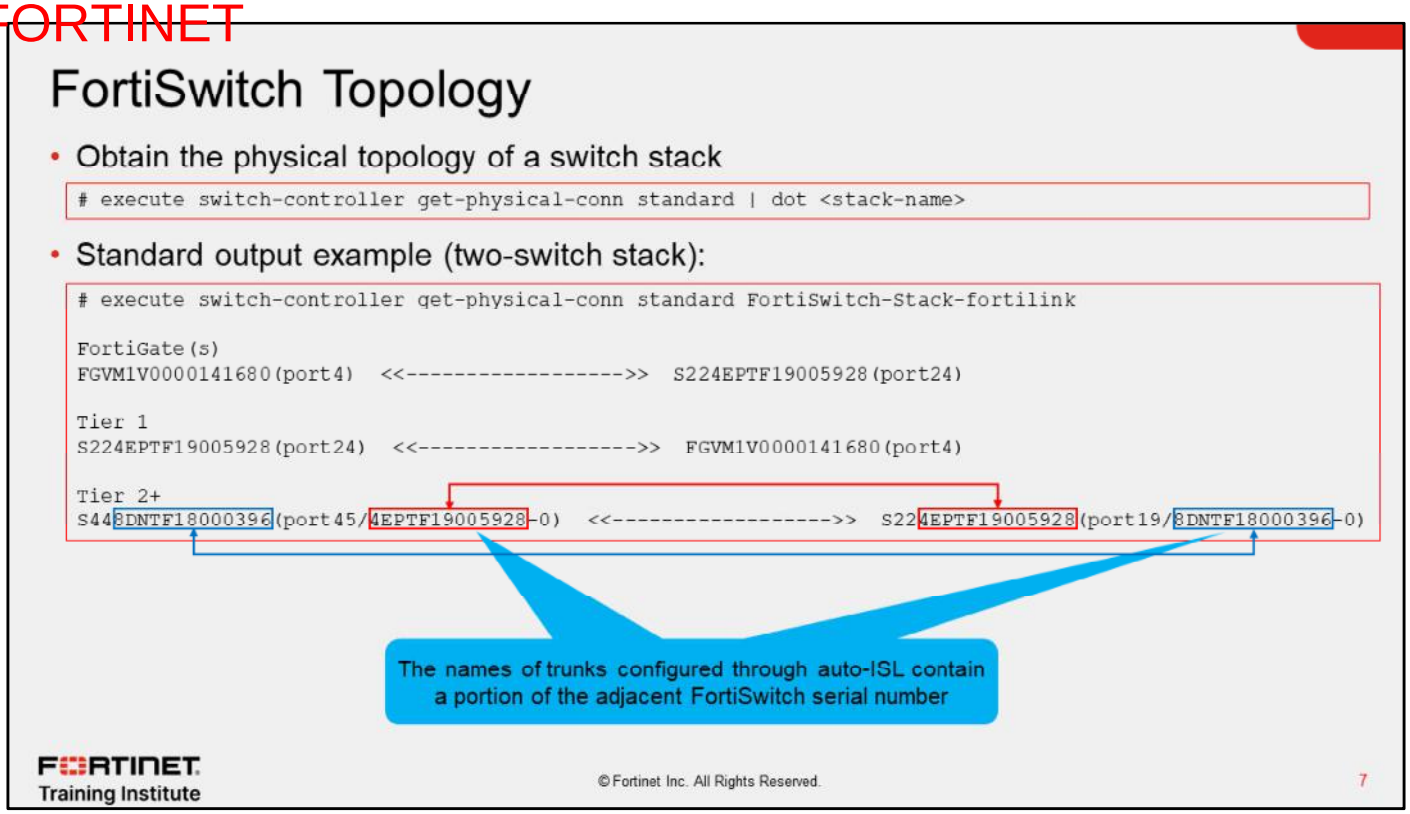
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can run the `execute switch-controller get-conn-status` command on the FortiSwitch CLI to display the managed FortiSwitch status. On FortiSwitch, the output of the command is more focused on the FortiGate side of the connection—the switch controller side.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The next step in troubleshooting a switch is probably getting the stack physical connection details. This is especially helpful when troubleshooting instability issues caused by incorrect physical connections.

You can get the current physical topology of your stack by running the `execute switch-controller get-physical-conn` command. The command can display the output in standard format or dot format. The standard format is more suited for small deployments, because the output for these cases is usually easier to read. The standard output organizes the switches per tier (or level), and indicates the ports used for every connection between switches, and between switches and FortiGate devices. For example, the standard format output shown on this slide corresponds to a two-switch stack. The switch that is directly connected to FortiGate is classified as tier 1.

In addition, the output also includes the names of the trunks automatically configured through auto-ISL. In auto-ISL, the trunk names contain a portion of the adjacent switch serial number.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Topology (Contd)

- Dot output example (two-switch stack):

```
# execute switch-controller get-physical-conn dot FortiSwitch-Stack-fortilink
digraph {

graph [layout = dot, rankdir = TB]

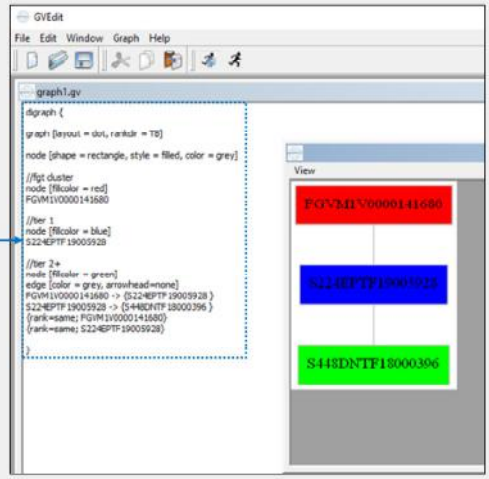
node [shape = rectangle, style = filled, color = grey]

//fgt cluster
node [fillcolor = red]
FGVM1V0000141680

//tier 1
node [fillcolor = blue]
S224EPTF19005928

//tier 2+
node [fillcolor = green]
edge [color = grey, arrowhead=none]
FGVM1V0000141680 -> {S224EPTF19005928 }
S224EPTF19005928 -> {S448DNTF18000396 }
{rank=same; FGVM1V0000141680}
{rank=same; S224EPTF19005928}

}
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

For large deployments, you may want to use the dot format output instead. The output can be loaded into an image editor that supports graphviz format, such as GVEdit, so the output is displayed as a graph. Alternatively, you can upload the output into a graphviz converter website such as `www.webgraphviz.com`, to generate the graph.

In the example shown on this slide, the dot output has been loaded into GVEdit. GVEdit then generates a graph depicting the physical topology of the stack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Synchronization Status

```
# execute switch-controller get-sync-status
all          Get FortiSwitch sync status.
group        Get FortiSwitch sync status by group.
name         Get FortiSwitch sync status by switch name.
switch-id    Get FortiSwitch sync status by switch.

# execute switch-controller get-sync-status all
Managed-devices in current vdom root:

FortiLink interface : fortilink
SWITCH (NAME)                          STATUS CONFIG          MAC-SYNC       HTTP-UPGRADE
S424DPTF20000027 (Core-1)              Up     Idle            Pending        (30%)
S424DPTF20000029 (Access-1)            Up     Synchronizing   Idle           Idle
S424DPTF20000051 (Core-2)              Up     Idle            Synchronizing  Idle
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

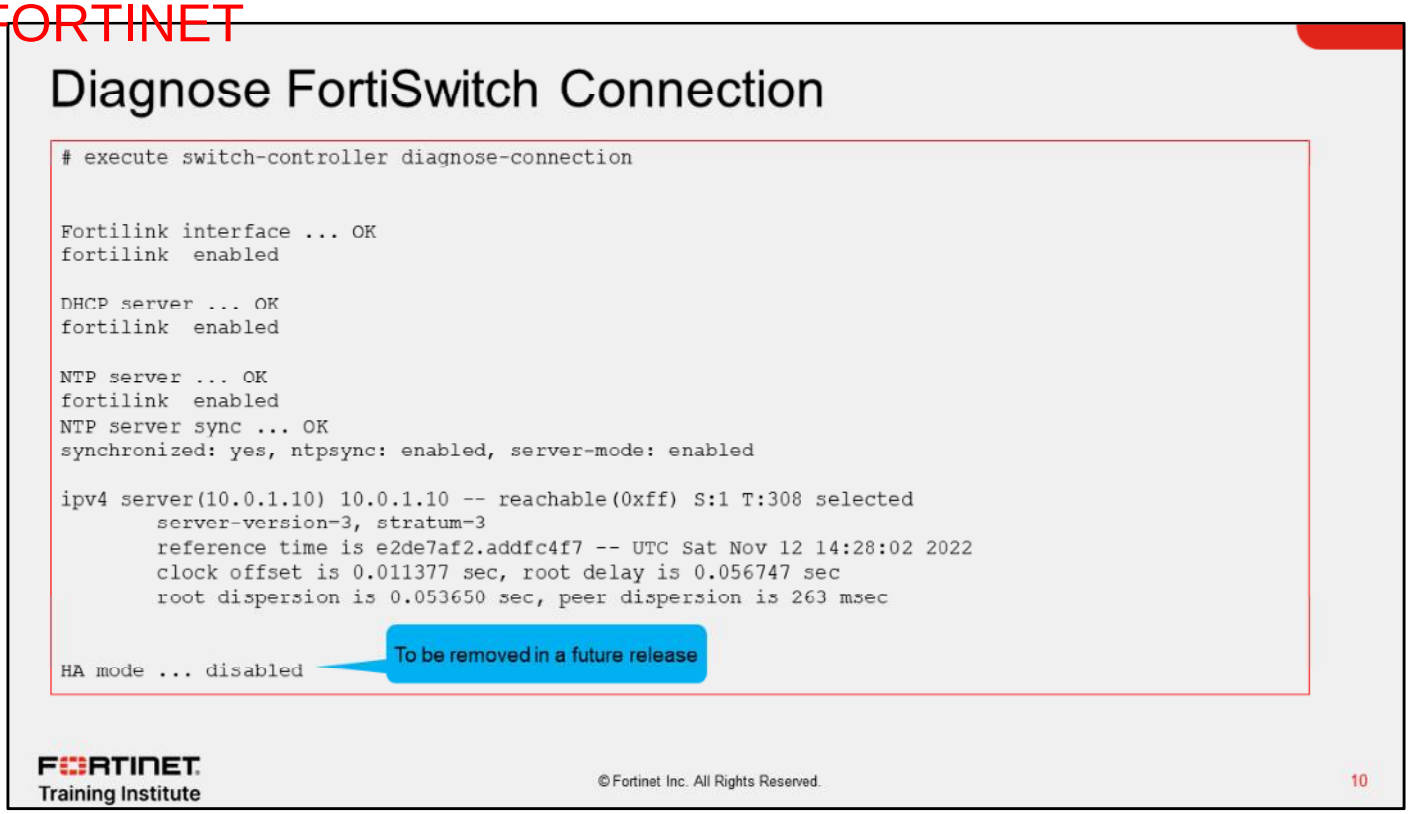
9

Each time you change the FortiSwitch configuration on FortiGate, the change is saved in the FortiGate configuration first, and then FortiGate pushes the configuration change to FortiSwitch through HTTPS and using the FortiSwitch REST API. FortiSwitch then saves the changes locally. The command `execute switch-controller get-sync-status` shows the configuration synchronization status between FortiGate and FortiSwitch.

The command also displays the MAC address synchronization and HTTP firmware upgrade status. FortiGate frequently polls the MAC address table from all managed switches to get the physical address listed on each port. This information is then used by FortiGate to provide visibility, control, and ultimately security of the network. In addition, FortiGate supports two methods for pushing firmware image files to managed switches: HTTPS and CAPWAP. HTTPS is the default method, and the upgrade status information displayed by the `execute switch-controller get-sync-status` command is for the HTTPS method *only*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



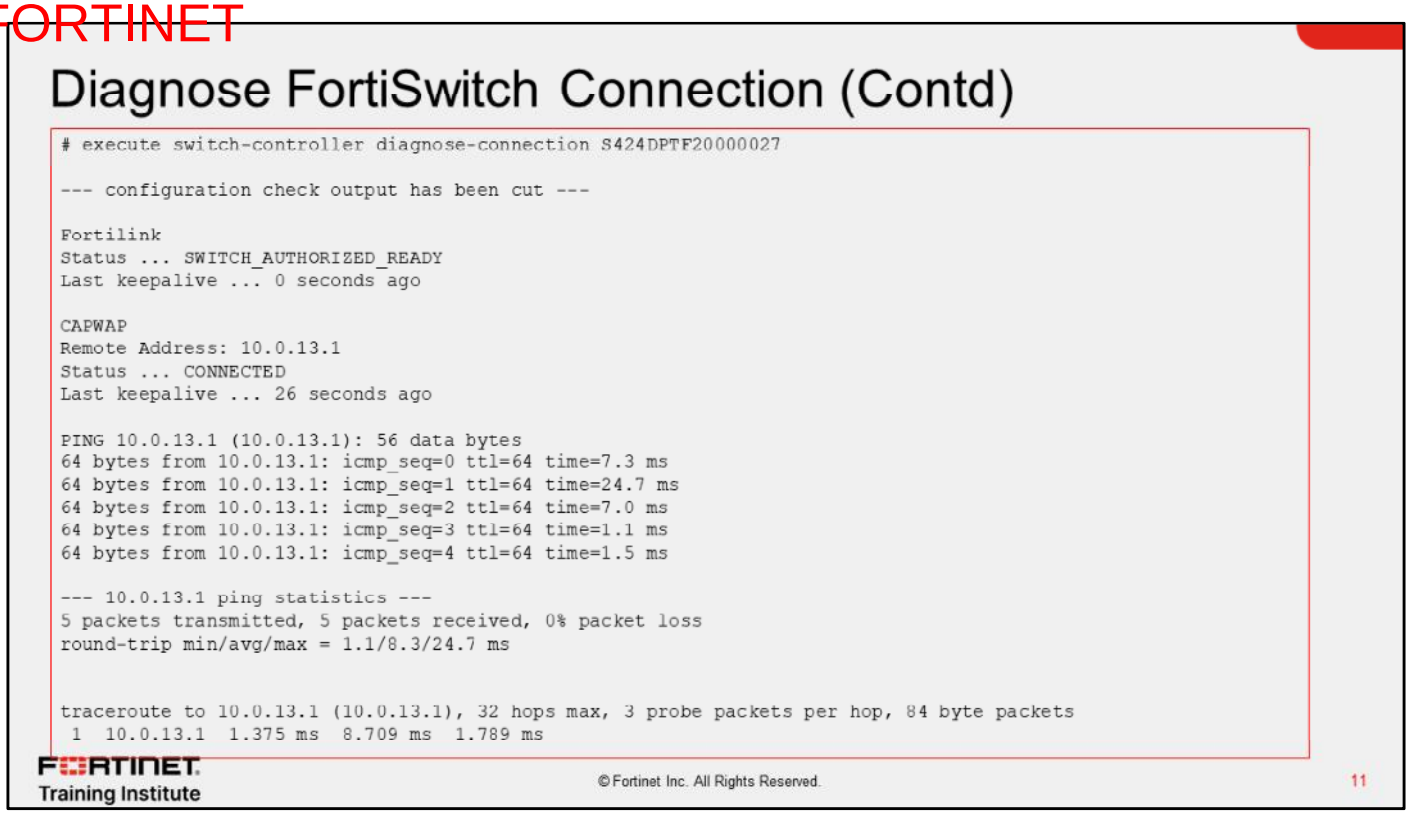
To verify that all the configuration needed for switch management is in place, you can run the `execute switch-controller diagnose-connection` command. FortiGate checks that the following settings are present:

- The FortiLink interface has the `fortilink` setting enabled
- There is a DHCP server scope for the FortiLink interface
- The NTP server is enabled on the FortiLink interface

The command also provides the latest NTP status information, as well as the FortiGate high availability (HA) mode in use. Note that the HA mode is irrelevant, because FortiSwitch can now be managed in both HA active-passive (A-P) and active-active (A-A) modes. For this reason, the output about the HA mode in use will be removed in a future release.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you specify a switch, the `execute switch-controller diagnose-connection` command also includes in the output the following connectivity checks between FortiGate and the switch:

- FortiLink and CAPWAP connection status, including the last keepalive (or heartbeat) received
- The results of pings FortiGate sends to the switch
- The detected hops resulting from a traceroute FortiGate performs

Note that this command also displays the output for the configuration check, which is described in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Managed Switch Communication Processes

- Processes involved in switch management:

Function	FortiGate Process Name	FortiSwitch Process Name
FortiLink discovery and heartbeats	fortilinkd	fortilinkd
CAPWAP	cu_acd	cu_swtpd
Configuration changes	flcfgd	httpsd

- To enable a real-time debug on FortiGate and FortiSwitch:

```
# diagnose debug application <process_name> <debug_level>
```

- To enable timestamps on debug messages on FortiGate and FortiSwitch:

```
# diagnose debug console timestamp enable
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

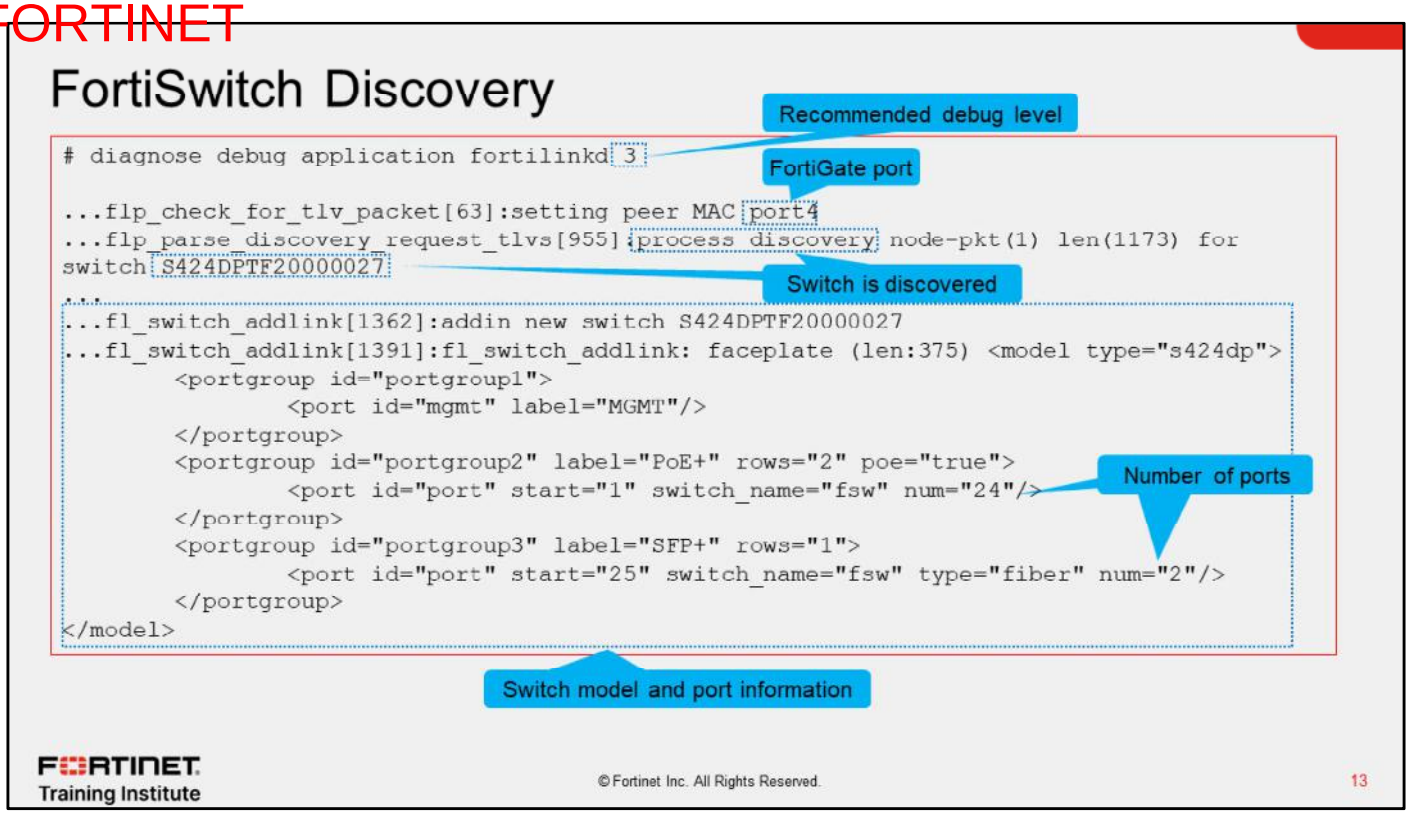
12

The table on this slide shows the processes that handle the discovery, heartbeats, and configuration changes on a managed FortiSwitch. The table includes the respective processes on both FortiGate and FortiSwitch.

You can use the same command on FortiGate and FortiSwitch to enable debug on a process, as shown on this slide. It is also recommended that you enable timestamps on debug messages. Timestamps make debug analysis much easier because it enables you to correlate events and identify related messages in the debug output.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



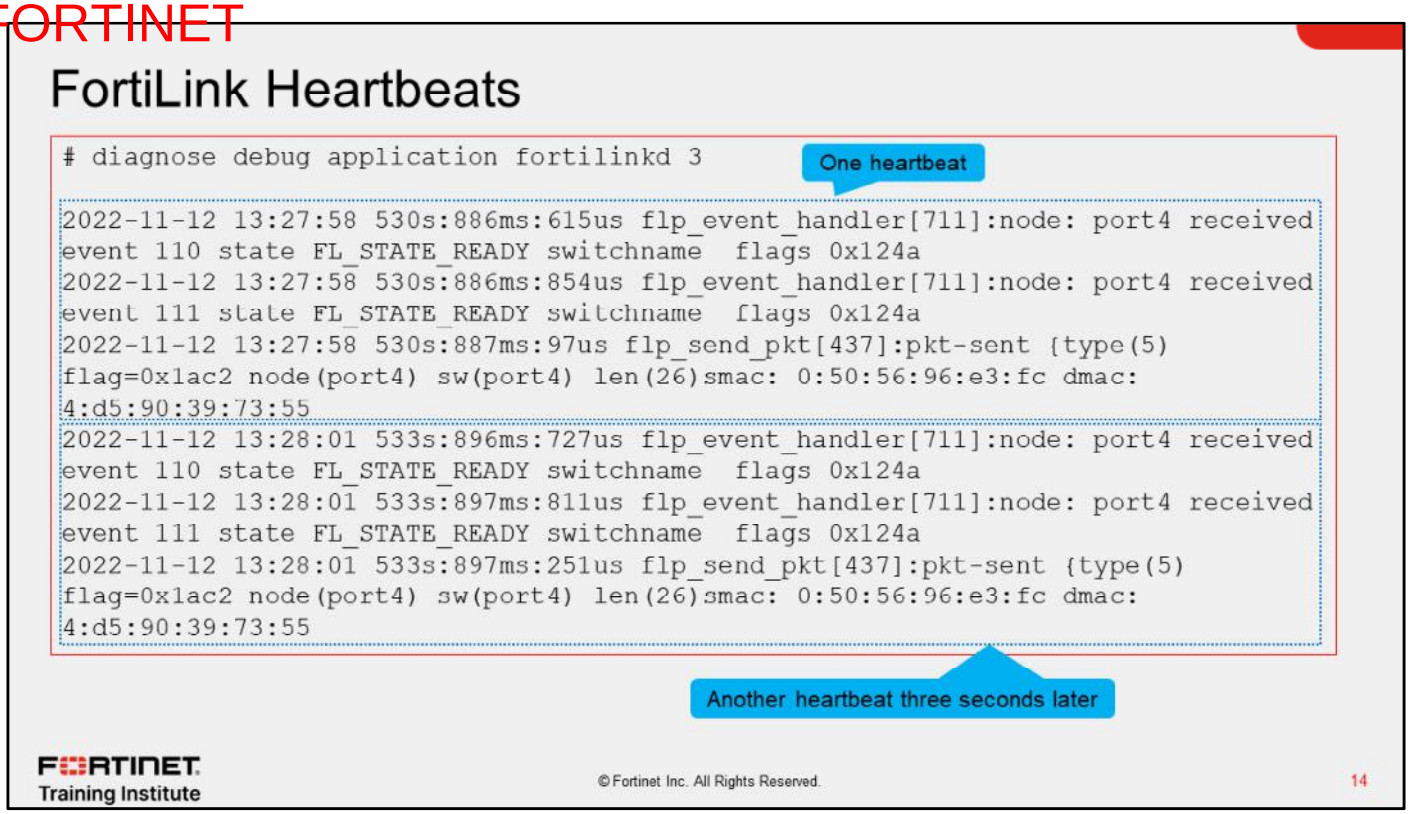
On FortiGate, you can enable the debug of the `fortilinkd` process for monitoring and troubleshooting the discovery of FortiSwitch devices.

When a new FortiSwitch is discovered, the debug output shows the FortiSwitch serial number, as well as the FortiGate port where the FortiLink frames that triggered the switch discovery were received.

In addition, because the FortiLink discovery frames include the switch port information, FortiGate reads this information from the frames to build the switch faceplate image shown on the GUI. The output on this slide shows that FortiGate discovered a FortiSwitch 424D-POE device that has three types of ports: MGMT (management), PoE+, and SFP+. When there are multiple ports of the same type, the output indicates the number of ports of that type.

Vouchers & Dumps are Available | WhatsApp +201224560923

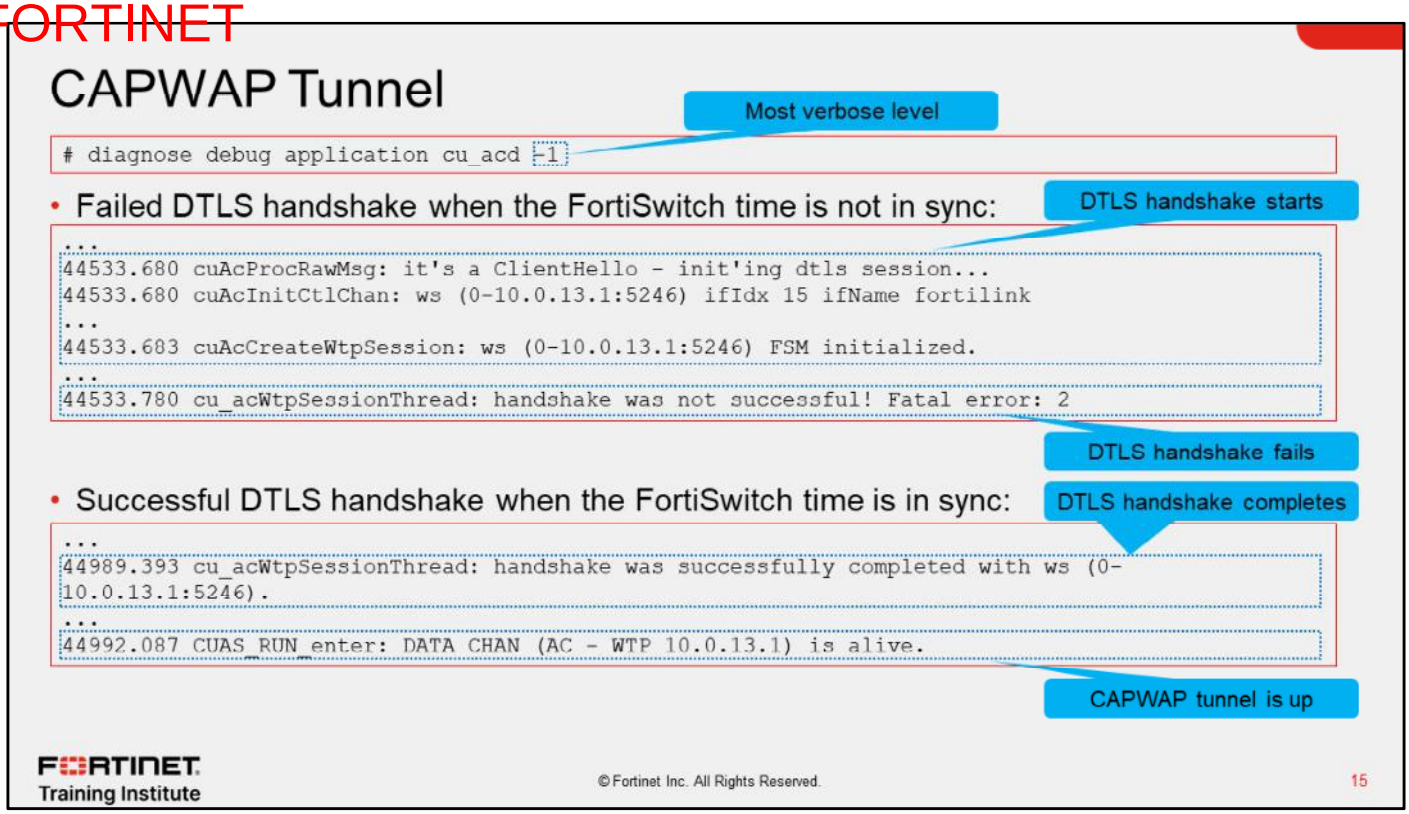
DO NOT REPRINT Brave-dumps.com
© FORTINET



After you authorize a switch and it comes online, the switch starts sending FortiLink heartbeats to FortiGate every three seconds. FortiGate then acknowledges the heartbeats by sending a reply to the switch. The debug output for the `fortilinkd` process will also show these heartbeats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

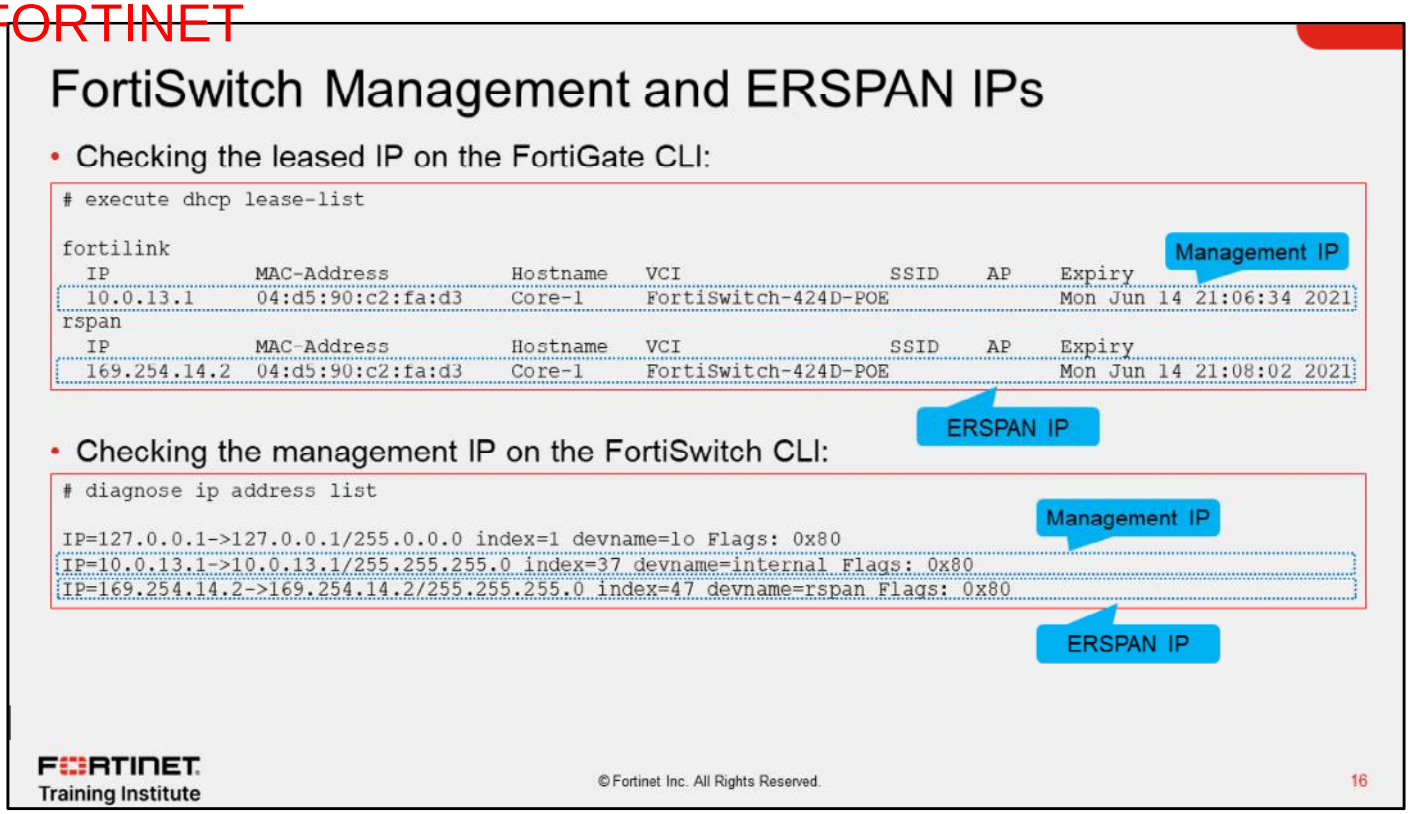


On FortiGate, you can enable debug of the `cu_acd` process to troubleshoot CAPWAP tunnel issues. The recommended verbosity level is `-1`, which is the most detailed level. For this reason, expect to see a considerable number of messages in the debug output.

The example on this slide shows key debug messages generated by `cu_acd` when the DTLS handshake in the CAPWAP tunnel fails, and when it is completed. In the example, the failed DTLS handshake is caused by the FortiSwitch time not being in sync with FortiGate. When the time is in sync, the DTLS handshake is completed and the CAPWAP tunnel comes up afterwards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you authorize a switch, the switch forms a direct or indirect trunk connection to FortiGate.

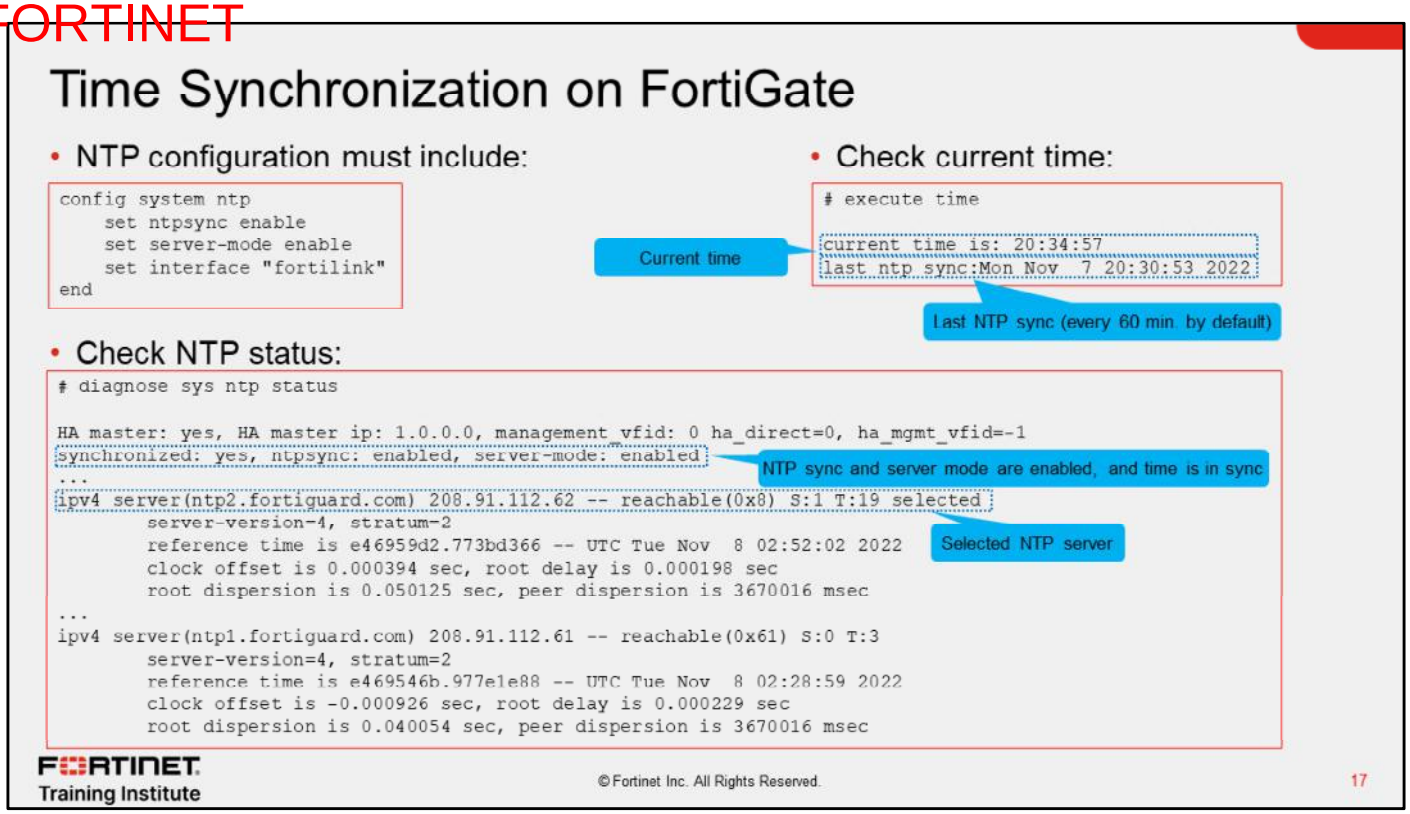
For a direct connection, FortiSwitch creates a FortiLink trunk. For an indirect connection, FortiSwitch creates an inter-chassis link (ICL) or a regular inter-switch link (ISL). After the trunk is formed, and there is Layer 2 connectivity between FortiGate and FortiSwitch, FortiSwitch requests from FortiGate two IP addresses through DHCP: the management IP and the encapsulated remote SPAN (ERSPAN) IP. The management IP is the IP address assigned to the FortiSwitch internal interface, and is used for all IP management communication between FortiGate and FortiSwitch.

ERSPAN enables FortiSwitch to encapsulate mirrored traffic into Generic Routing Encapsulation (GRE) and send it across a Layer 3 network. The ERSPAN IP is used as the source IP address of the GRE packets. You will learn more about ERSPAN in this lesson.

On FortiGate, you can verify that FortiGate leased the IP addresses to FortiSwitch by running the `execute dhcp lease-list` command. On FortiSwitch, you can run the `diagnose ip address list` command to display the assigned IP addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



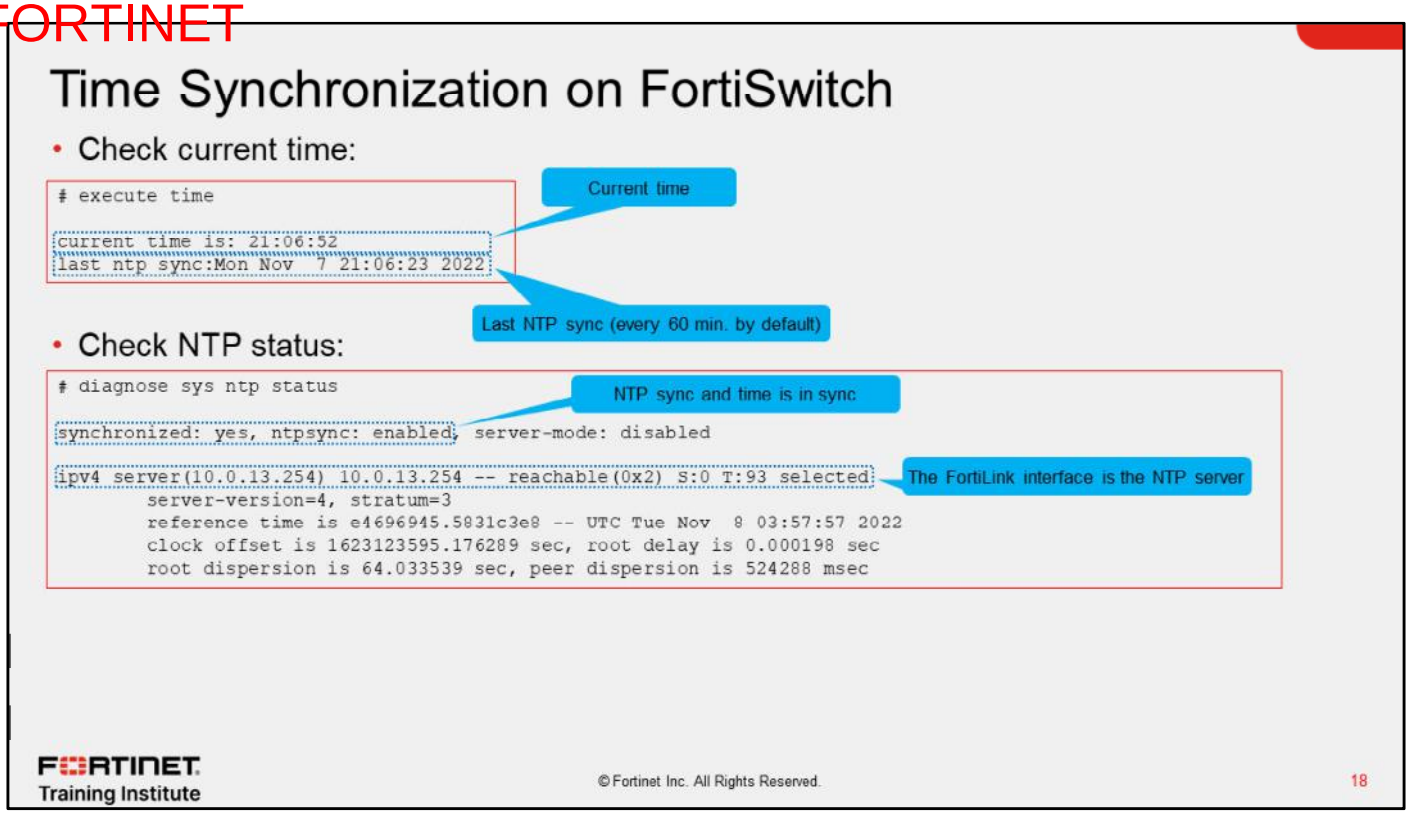
Time synchronization is critical in switch management. If the time on FortiGate and FortiSwitch is not synchronized, FortiSwitch can't complete the DTLS handshake used in CAPWAP, which prevents the switch from connecting to FortiGate. Another reason to have a working setup for time synchronization is because FortiSwitch doesn't retain its time after a reboot. When FortiSwitch is rebooted, the time on the switch is reset to the Unix epoch time (midnight of January 1, 1970, UTC).

The first step to check time synchronization is by checking the NTP system configuration on FortiGate. The example on this slide shows the settings that must be present in the NTP system configuration node. After that, you can check the NTP status on FortiGate by running `diagnose sys ntp status`. The output should indicate that the time is synchronized, that NTP synchronization is enabled, and that server mode is enabled. The output should also indicate the selected NTP server by FortiGate to synchronize its time.

You can also run the `execute time` command to display the current system time, as well as the last time the time was synchronized using NTP. Note that by default, NTP time synchronization takes place every 60 minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

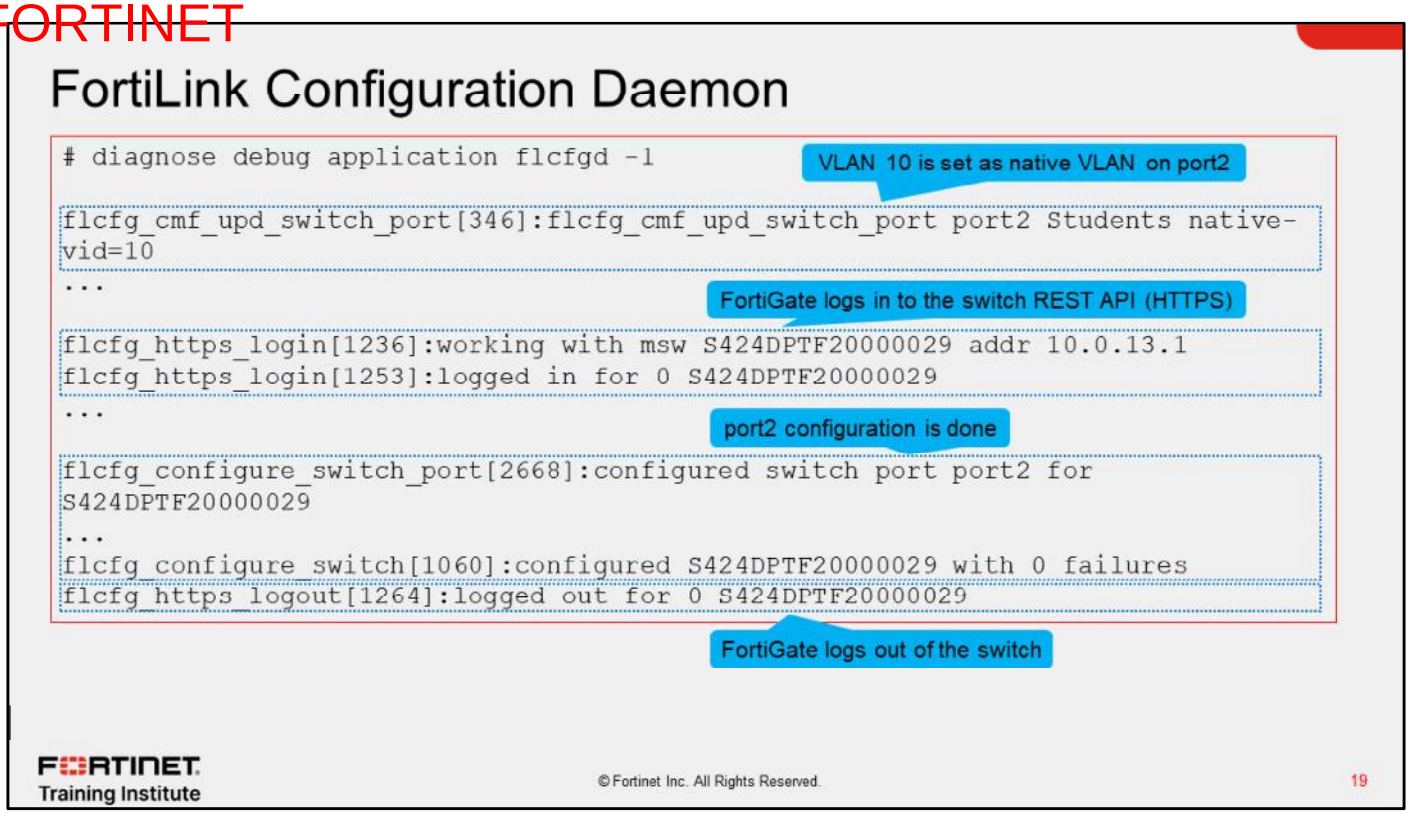
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To check the time on FortiSwitch, you use the same commands that you use on FortiGate. In the output of `diagnose sys ntp status`, you should see the FortiLink interface as the NTP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

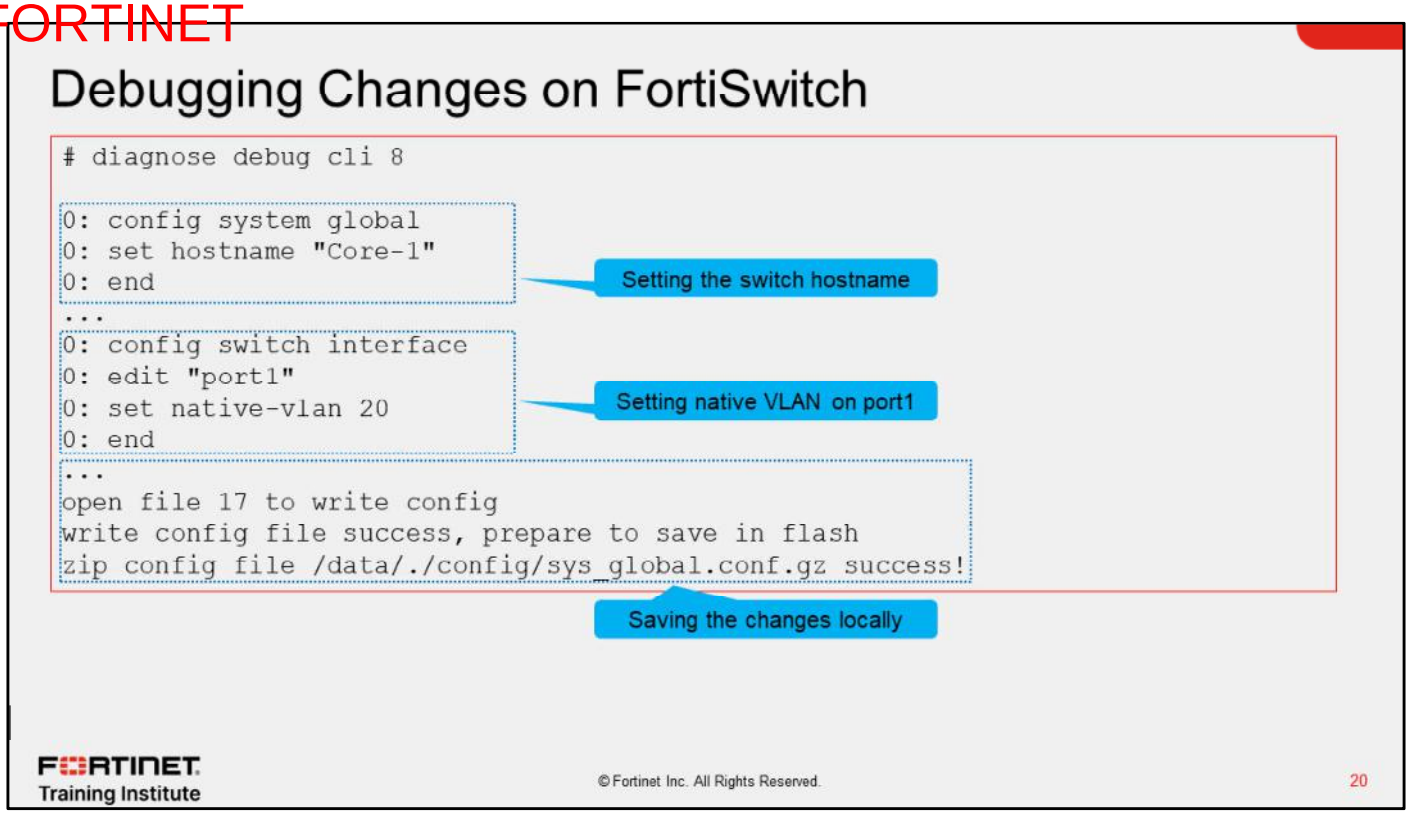


If you want to troubleshoot or monitor the configuration changes applied by FortiGate to the switches, you can enable debug for the FortiLink configuration daemon.

In the example shown on this slide, the administrator sets the native VLAN for `port2` on the switch to `Students`. The `Students` VLAN uses VLAN ID 10. Because the change is made on FortiGate, it triggers a configuration push to the managed switch. FortiGate first logs in to the managed switch REST API through HTTPS, and then applies the configuration changes required for port2. After it finishes applying the changes, FortiGate logs out of the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



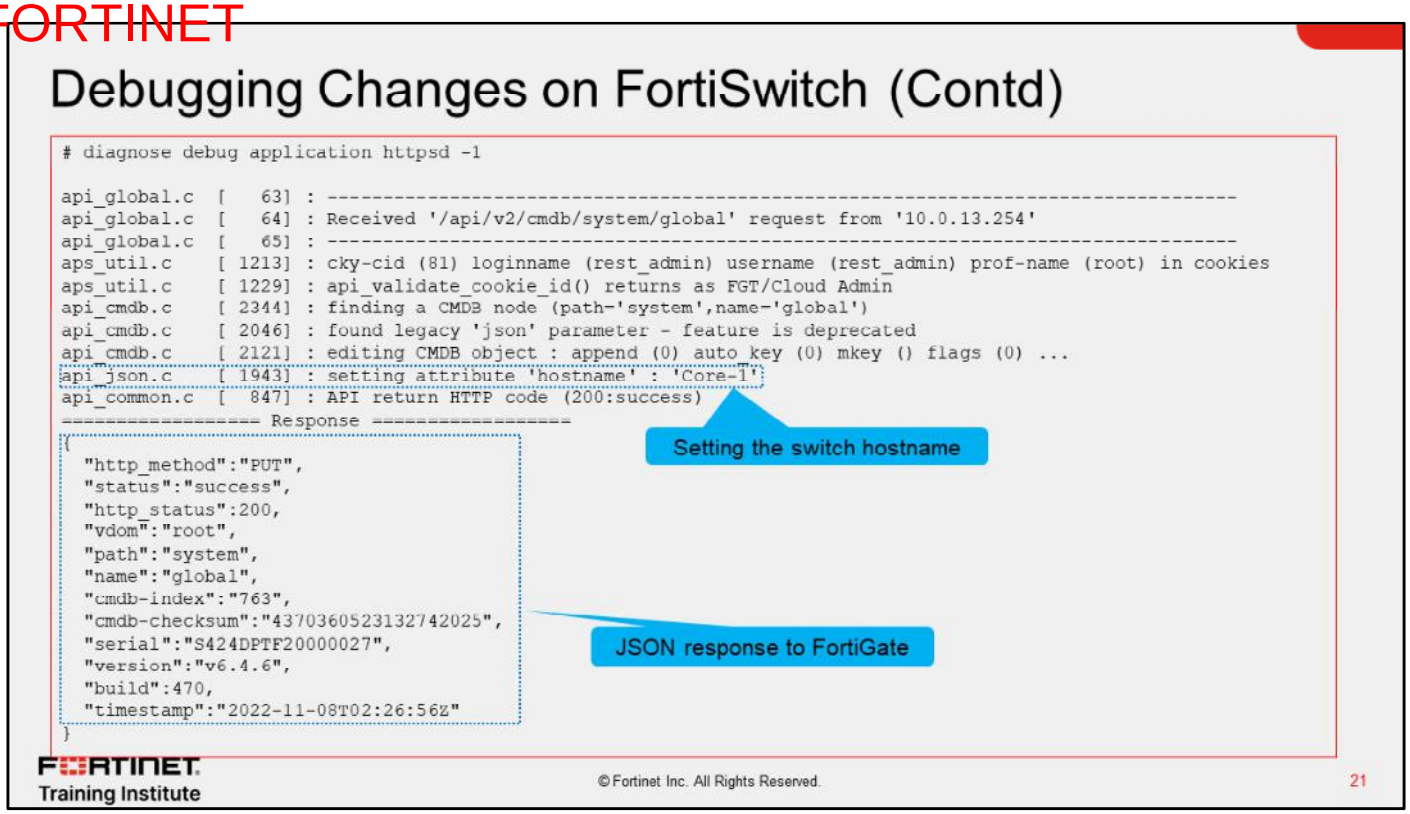
If you are facing configuration sync issues, you may want to track on FortiSwitch, the settings that FortiGate pushes to the device. One way to do this is by enabling the CLI debug on FortiSwitch, as shown on this slide.

When FortiGate pushes the configuration to FortiSwitch, FortiSwitch receives the changes through the REST API. After that, FortiSwitch applies the received settings to the local configuration using CLI commands. Enabling the CLI debug enables you to track these CLI commands and, as a result, identify any errors returned by the CLI when the commands are applied.

The example on this slide shows two configuration changes pushed by FortiGate. The first change sets the device hostname to `Core-1`, and the second sets VLAN 20 as the native VLAN on `port1`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSwitch receives configuration change requests through the REST API. On FortiSwitch, you can debug the messages exchanged over the REST API to identify change requests, as well as other management operations, by enabling debug for the `httpsd` process, as shown on this slide.

The example on this slide shows the `httpsd` debug for the same hostname change that was tracked using the CLI debug. Messages exchanged over the REST API use the JavaScript Object Notation (JSON) format. The `httpsd` debug shown on this slide also displays the FortiSwitch JSON response details sent to FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiOS process is responsible for pushing the configuration to FortiSwitch?
   - ✓ A. flcfgd
   - B. fortilinkd

2. Why is time synchronization critical in switch management?
   - A. It enables FortiGate to discover FortiSwitch.
   - ✓ B. It enables the CAPWAP tunnel to come up.

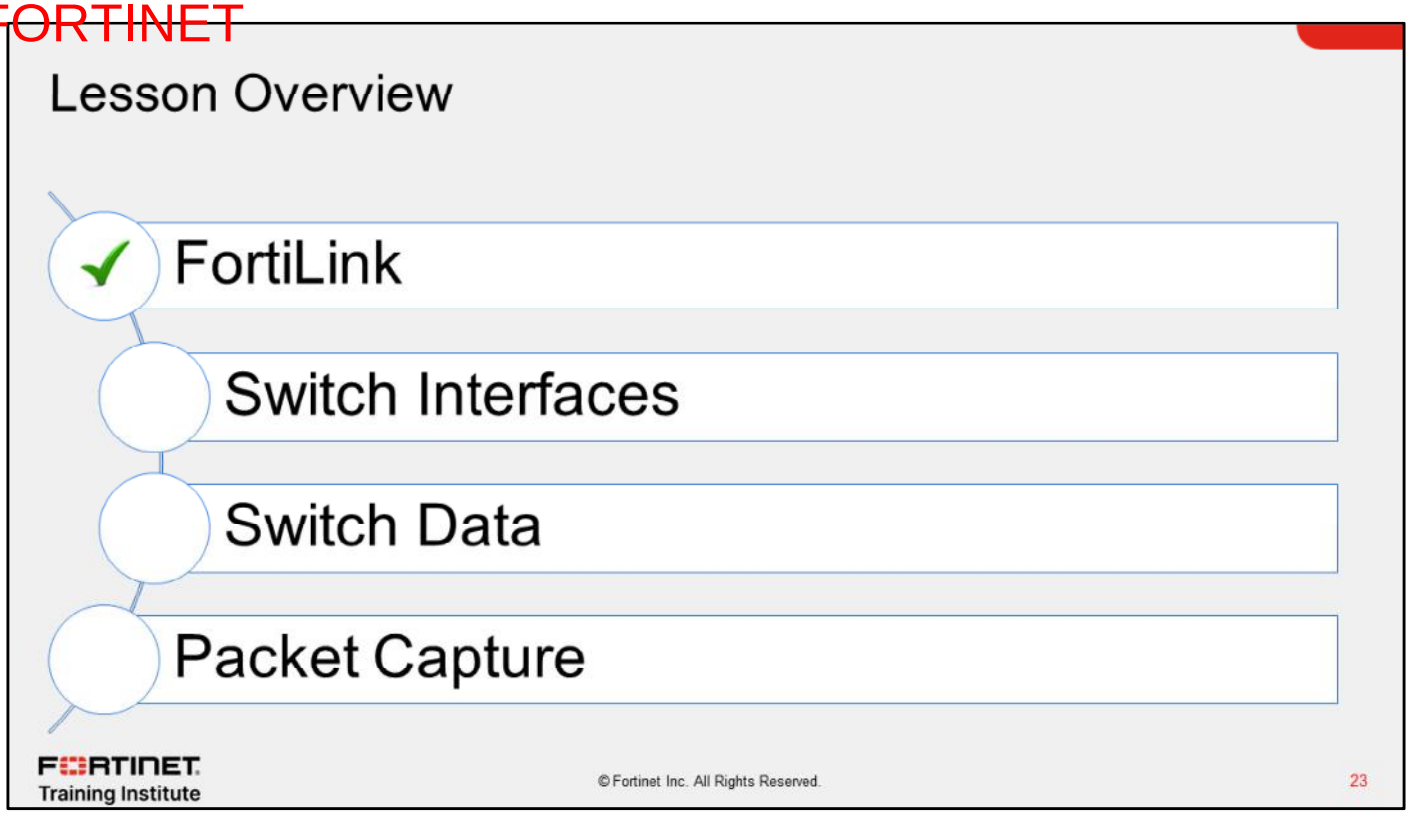
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

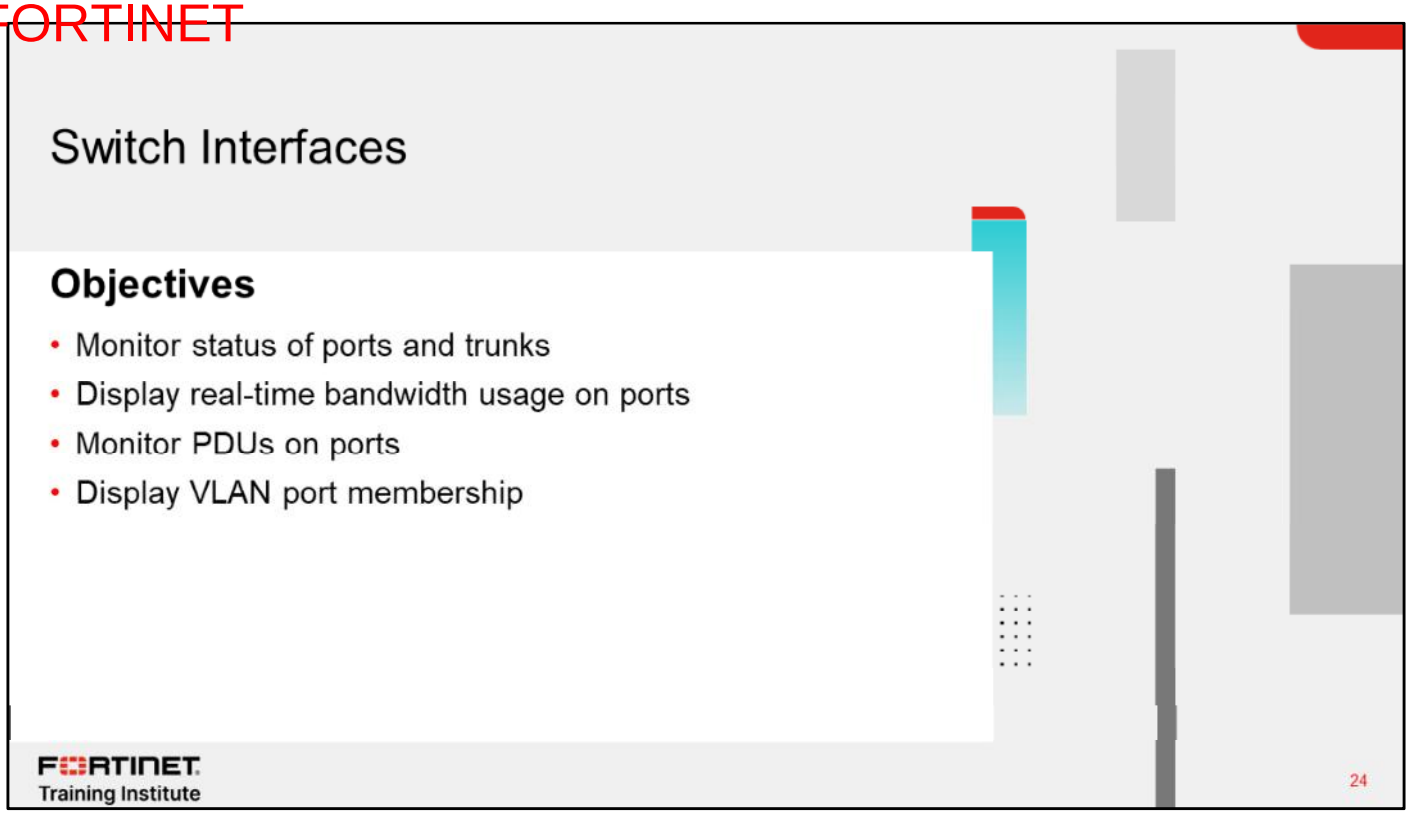


Good job! You now understand FortiLink troubleshooting.

Now, you will learn about troubleshooting switch interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in troubleshooting switch interfaces, you should be able to solve issues involving ports and trunks on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Checking the Status of Physical Ports

- On the FortiGate CLI:

```
# execute switch-controller get-conn-status <switch-id>
```

- On the FortiSwitch CLI:

Native VLAN on the port

```
# diagnose switch physical-ports summary

  Portname    Status  Tpid  Vlan  Duplex  Speed  Flags         Discard
  _________   ______  ____  ____  ______  _____  ____________  _________

  port1       down    8100  20    half    1G     QS,   ,       none
...
  port23      up      8100  4094  full    1G     QS,TS,        none
  port24      up      8100  4094  full    1G     QS,TS,        none
...
  internal    up      8100  4094  full    1G     QS,   ,       none

  Flags: QS(802.1Q) QE(802.1Q-in-Q,external) QI(802.1Q-in-Q,internal)
  TS(static trunk) TF(forti trunk) TL(lacp trunk); MD(mirror dst)
  MI(mirror ingress) ME(mirror egress) MB(mirror ingress and egress) CF (Combo Fiber), CC (Combo Copper)
LL(LoopBack Local) LR(LoopBack Remote)
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

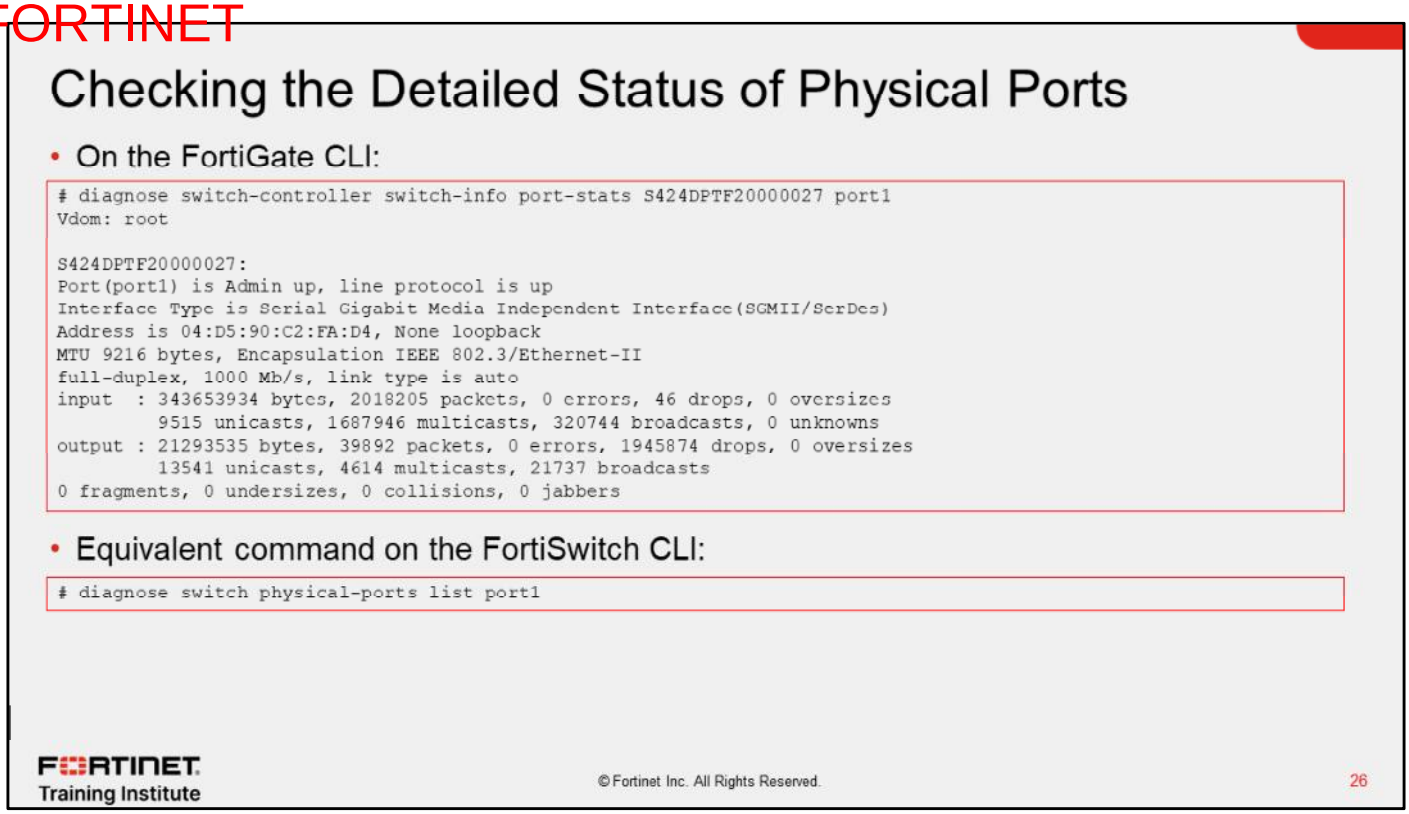
25

The example on this slide shows the commands that display a status summary of the physical ports on FortiSwitch. The output of `execute switch-controller get-conn-status` is described in this training.

The `diagnose switch physical-ports summary` command is available on the FortiSwitch CLI. The command output includes important information about physical switch ports only, including the `internal` interface. Note that the `Vlan` column refers to the native VLAN set on the port.

Vouchers & Dumps are Available | WhatsApp +201224560923

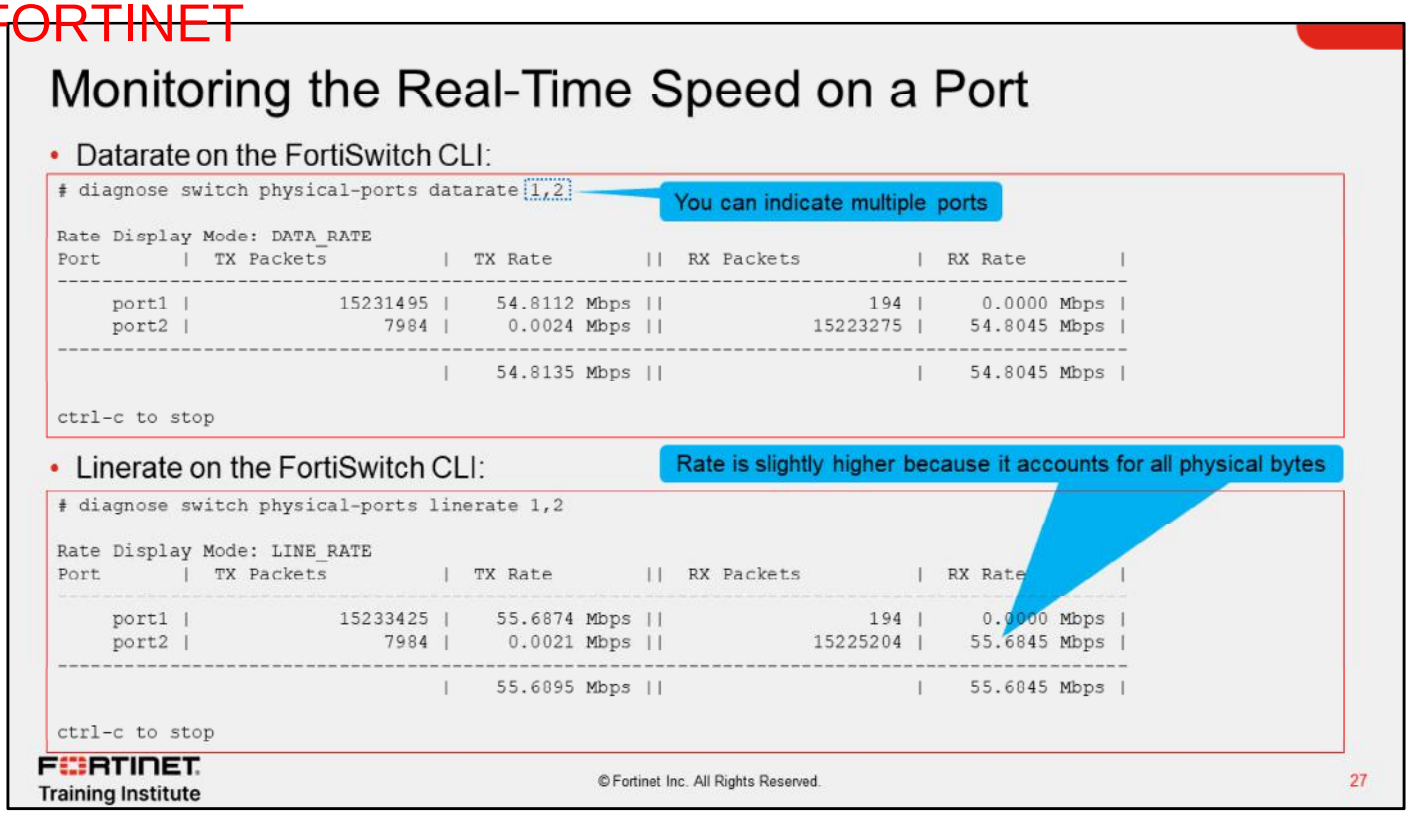
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiGate and FortiSwitch CLI commands shown on this slide produce the same output for a given port. The output includes advanced information such as the port maximum transmission unit (MTU), MAC address, and counters. The output is useful when troubleshooting more complex issues on FortiSwitch ports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

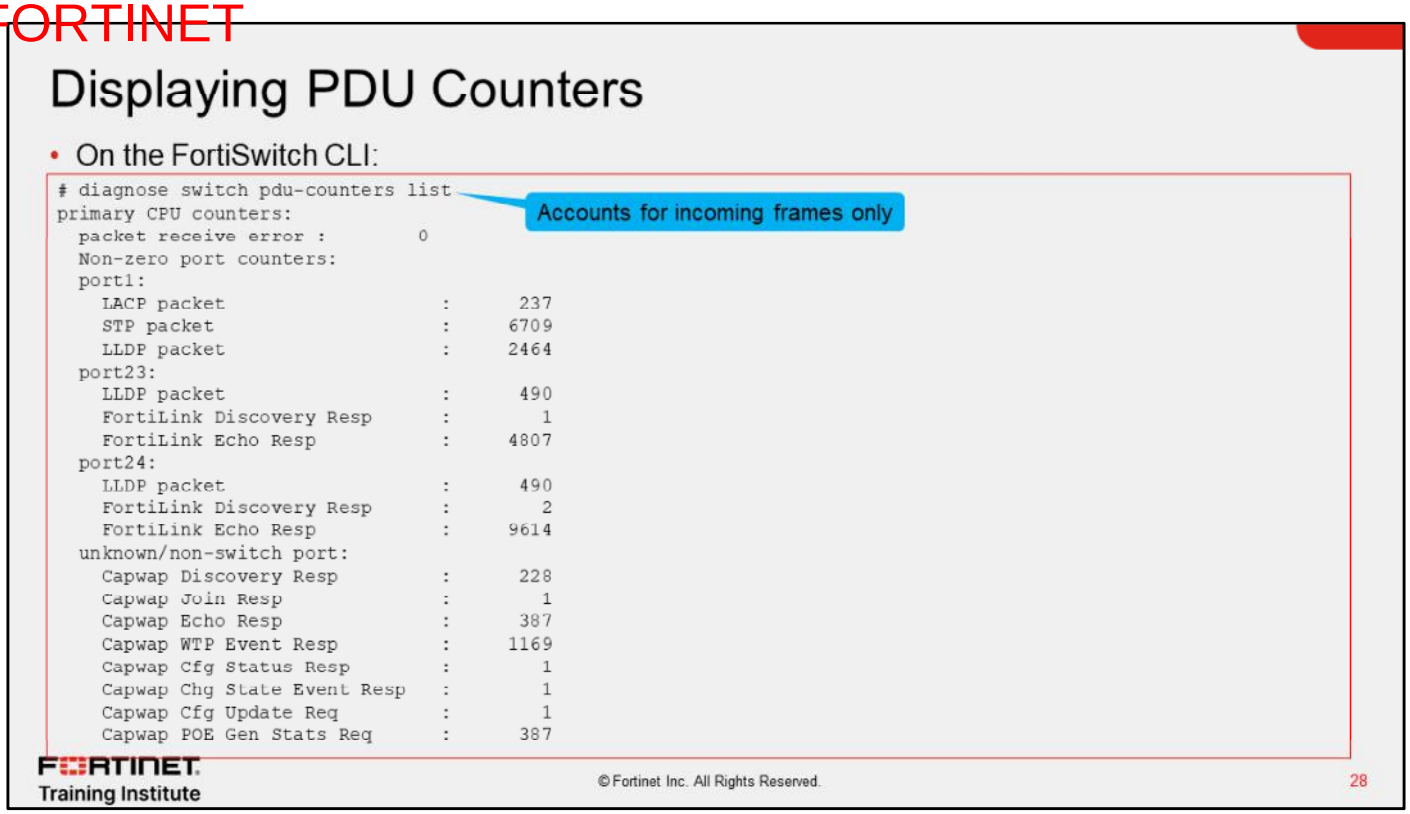


You can use the FortiSwitch `diagnose switch physical-ports datarate` and `diagnose switch physical-ports linerate` commands to get the real-time bandwidth usage on one or more ports. The speeds and number of packets displayed by both commands should be similar. However, the speed displayed by the `linerate` command should be slightly higher than the speed shown by the `datarate` command because FortiSwitch considers all physical bytes on the frame when calculating the speed for the `linerate` command. For example, when calculating the speed for the `linerate` command, FortiSwitch accounts for the frame check sequence (FCS) on the frame, which is not the case of the `datarate` command.

Note that there is no equivalent FortiOS command to display the data and line rates for a managed switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



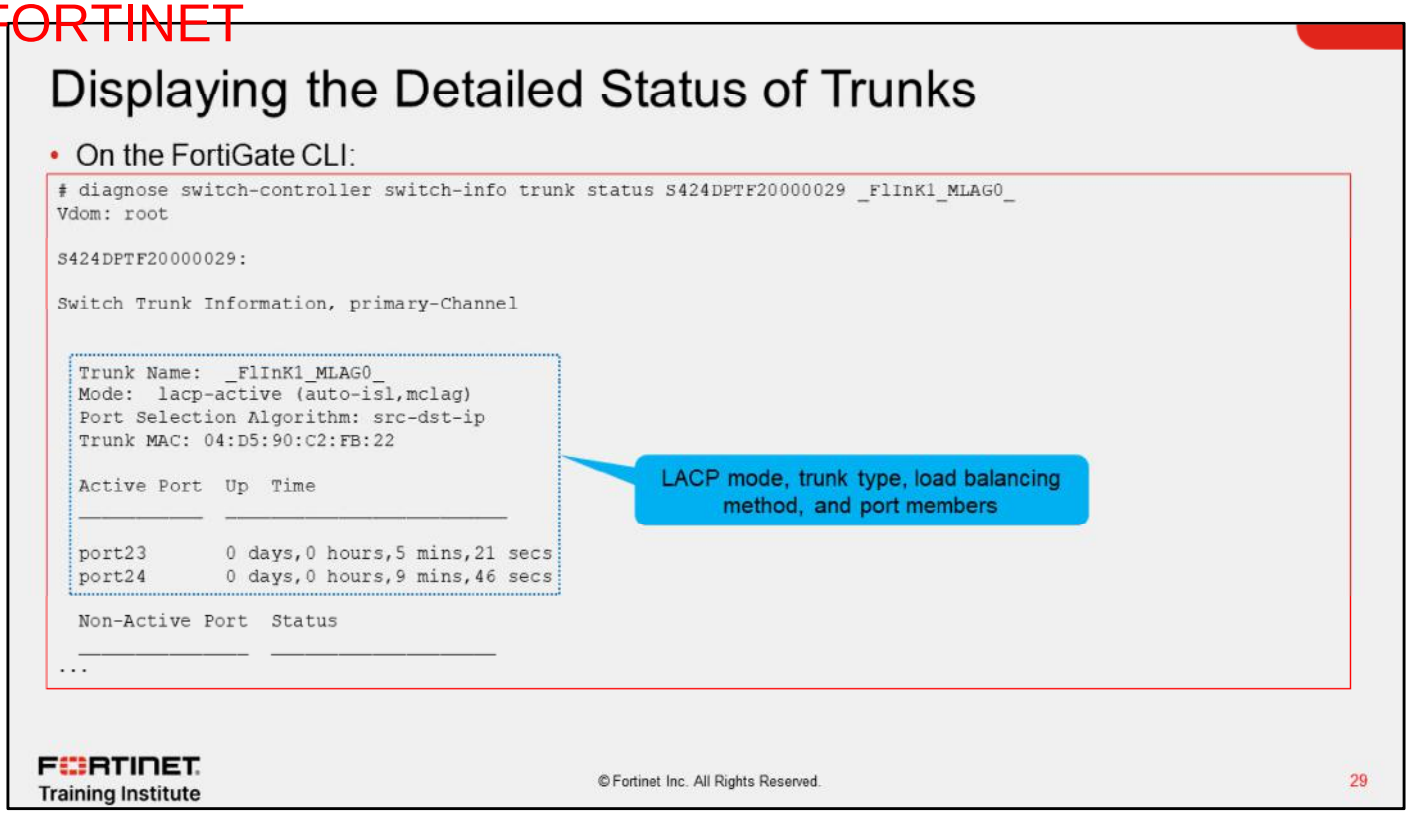
When troubleshooting issues involving protocols such as FortiLink, LLDP, STP, LACP, and CAPWAP, you may want to know if a given port at least received the frame for the problematic protocol. While you can capture ingress traffic to check the frame details on a port, an easier way is to check the protocol data unit (PDU) counters on the FortiSwitch CLI, as shown on this slide.

The output provided by the command displays the PDU types received on a port. For example, you can confirm that the FortiLink frames sent by FortiGate are received on a port by verifying that the corresponding PDU counter on the port increments. Similarly, you can confirm that BPDUs from the adjacent switch are received on a port by verifying that the STP counter on the port increments, and so on.

Note that the PDU counters account for ingress traffic only, not egress. Also note that there is no equivalent FortiOS command to display the PDU counters for a managed switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

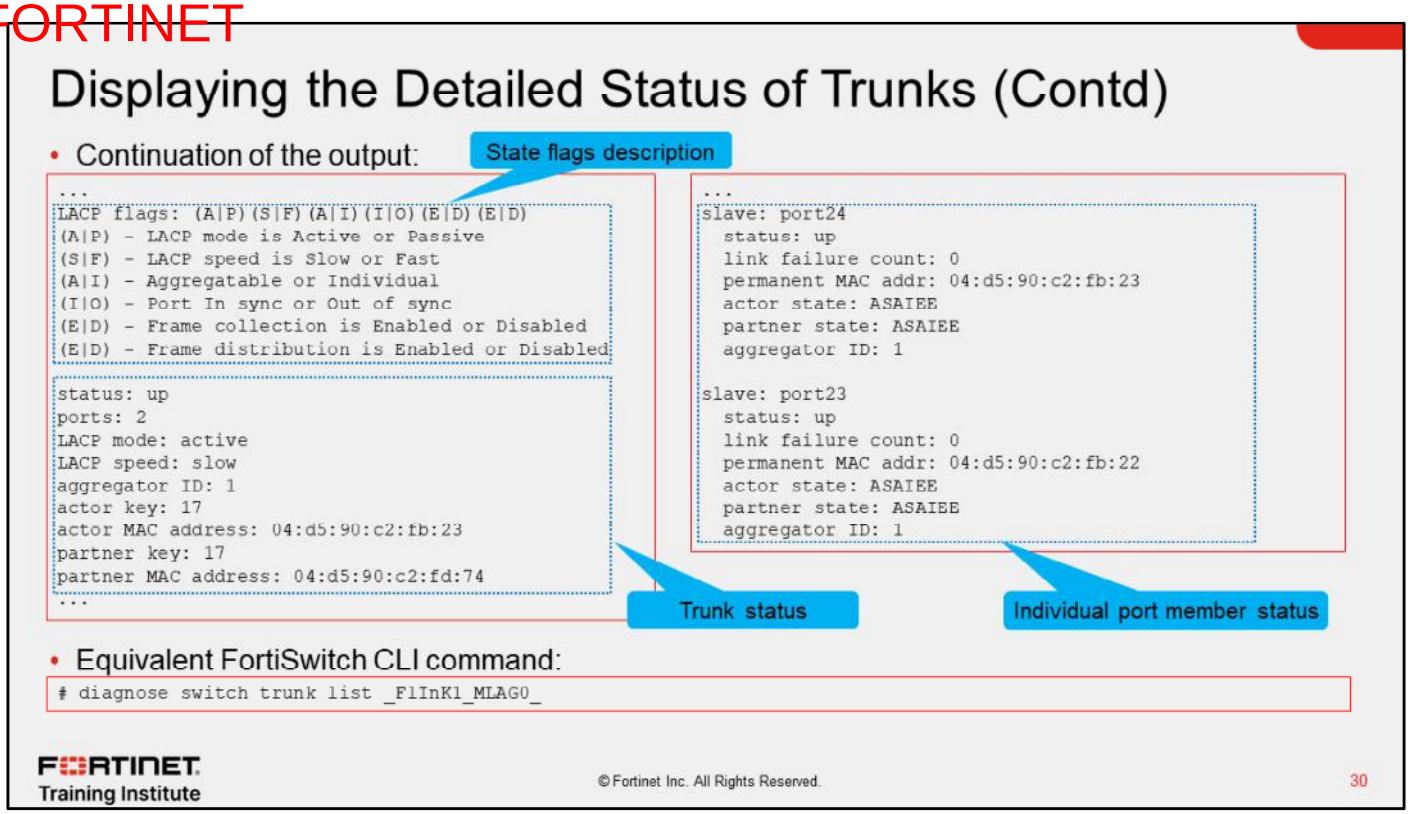


You can use the command shown on this slide to get a detailed status of a trunk on a managed FortiSwitch. The output starts by indicating the LACP mode in use (active, passive, or static), and whether the trunk is an auto-ISL trunk. If the trunk is an auto-ISL trunk, the output also indicates the auto-ISL trunk type: ICL or MCLAG.

Another important piece of information to look at is the port selection algorithm (or load balancing method) in use, as well as the trunk port members.

Vouchers & Dumps are Available | WhatsApp +201224560923

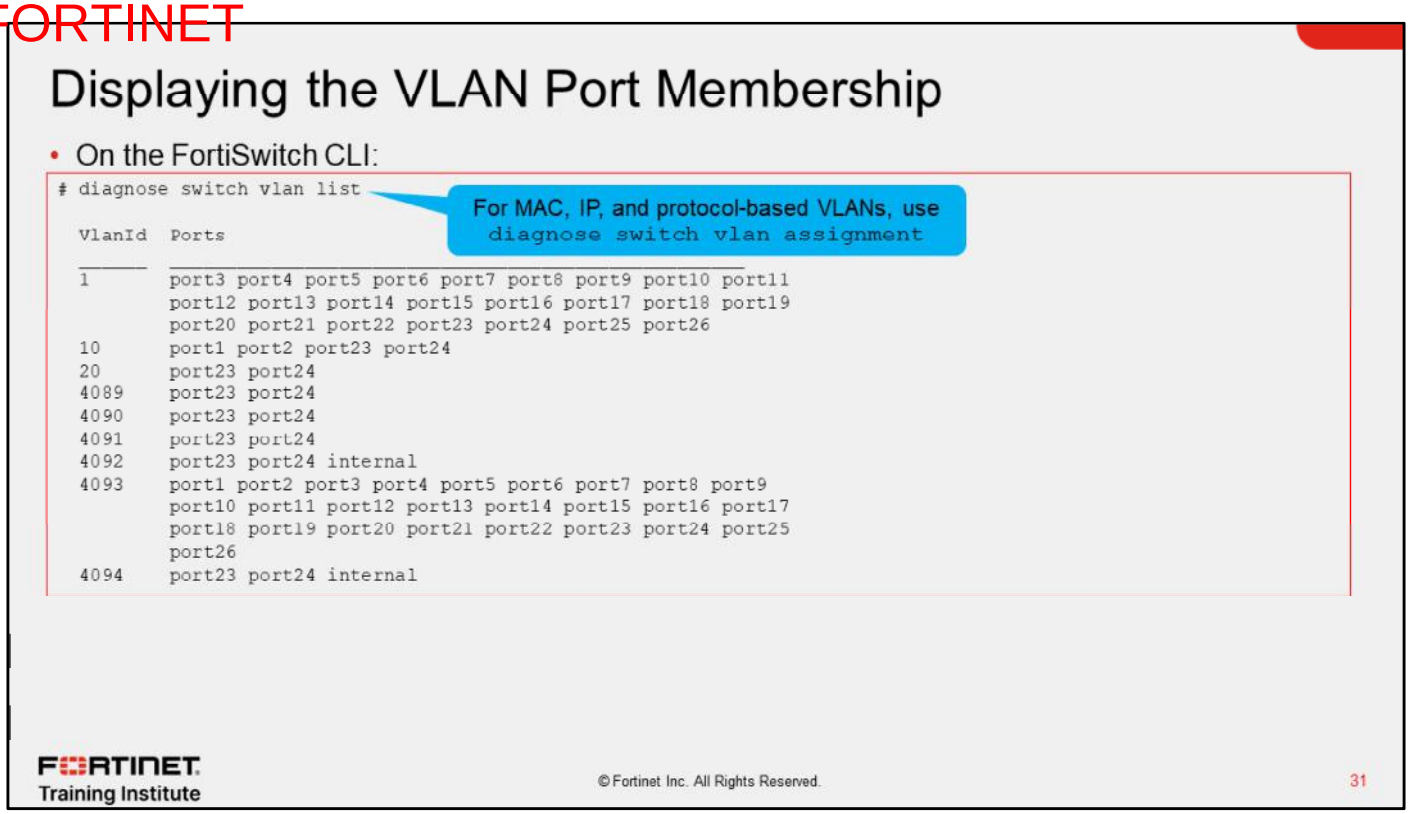
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a continuation of the output of the previous slide. The output shows the LACP flags description for your reference, the trunk status, as well as the individual port member status. Note that for a trunk to be up, at least one of its port members must be up.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are not using MAC, IP, and protocol-based VLANs, you can use the command on this slide to get the VLAN port membership on FortiSwitch. A port is considered part of a VLAN when the VLAN is set as the native VLAN on the port, or when the VLAN is included in the allowed VLANs on the port. For this reason, a port can be part of multiple VLANs.

Note that there isn't an equivalent FortiOS command that provides you with the same output. Also note that if you are using MAC, IP, and protocol-based VLANs, then you must use the `diagnose switch vlan assignment` command to get the VLAN assignments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiSwitchOS command displays the overall status of physical ports on the switch?

A. `execute switch-controller get-conn-status <switch-id>`
✓ B. `diagnose switch physical-ports summary`

2. Which command reports a slightly higher real-time bandwidth utilization on ports?

A. `diagnose switch physical-ports datarate`
✓ B. `diagnose switch physical-ports linerate`

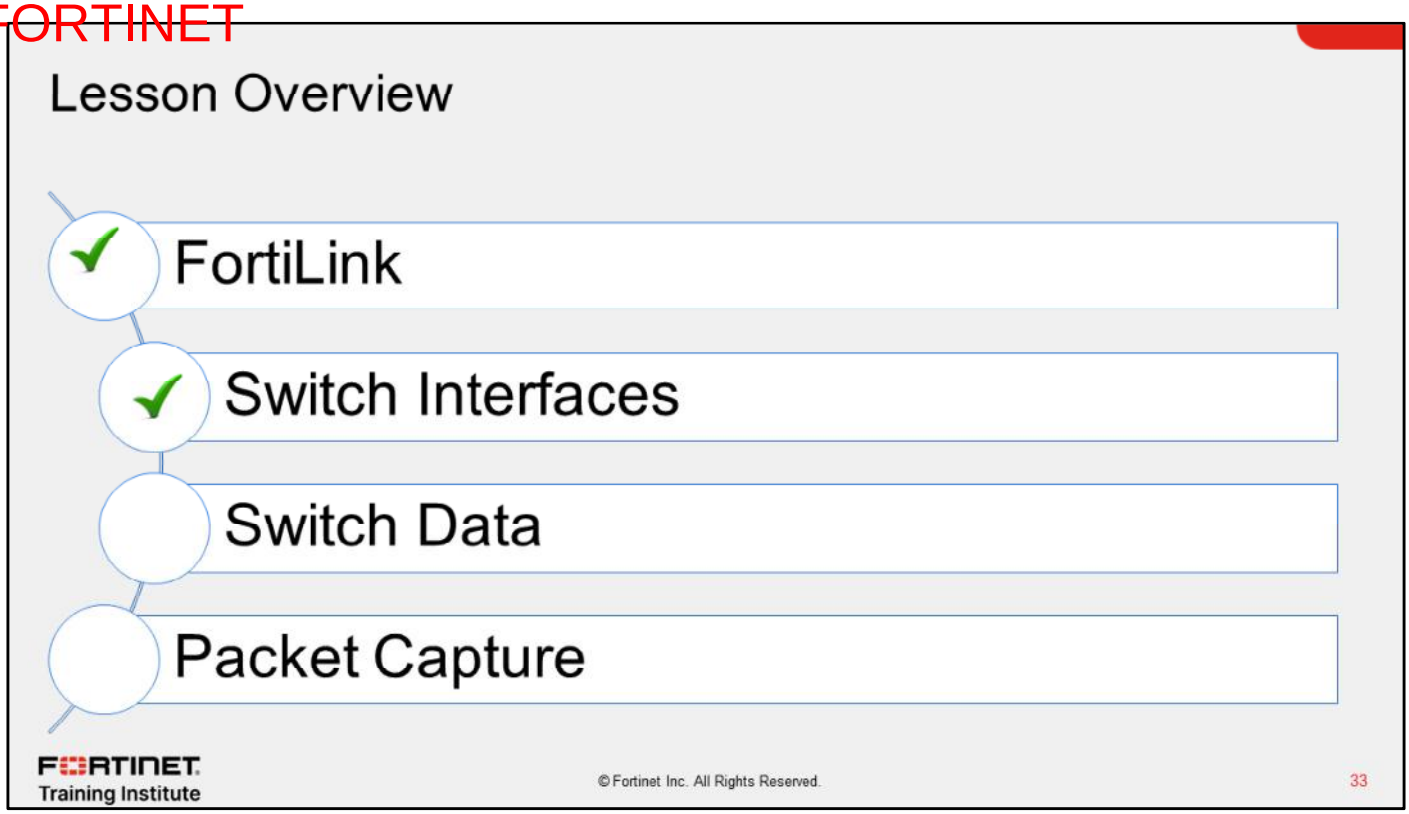
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

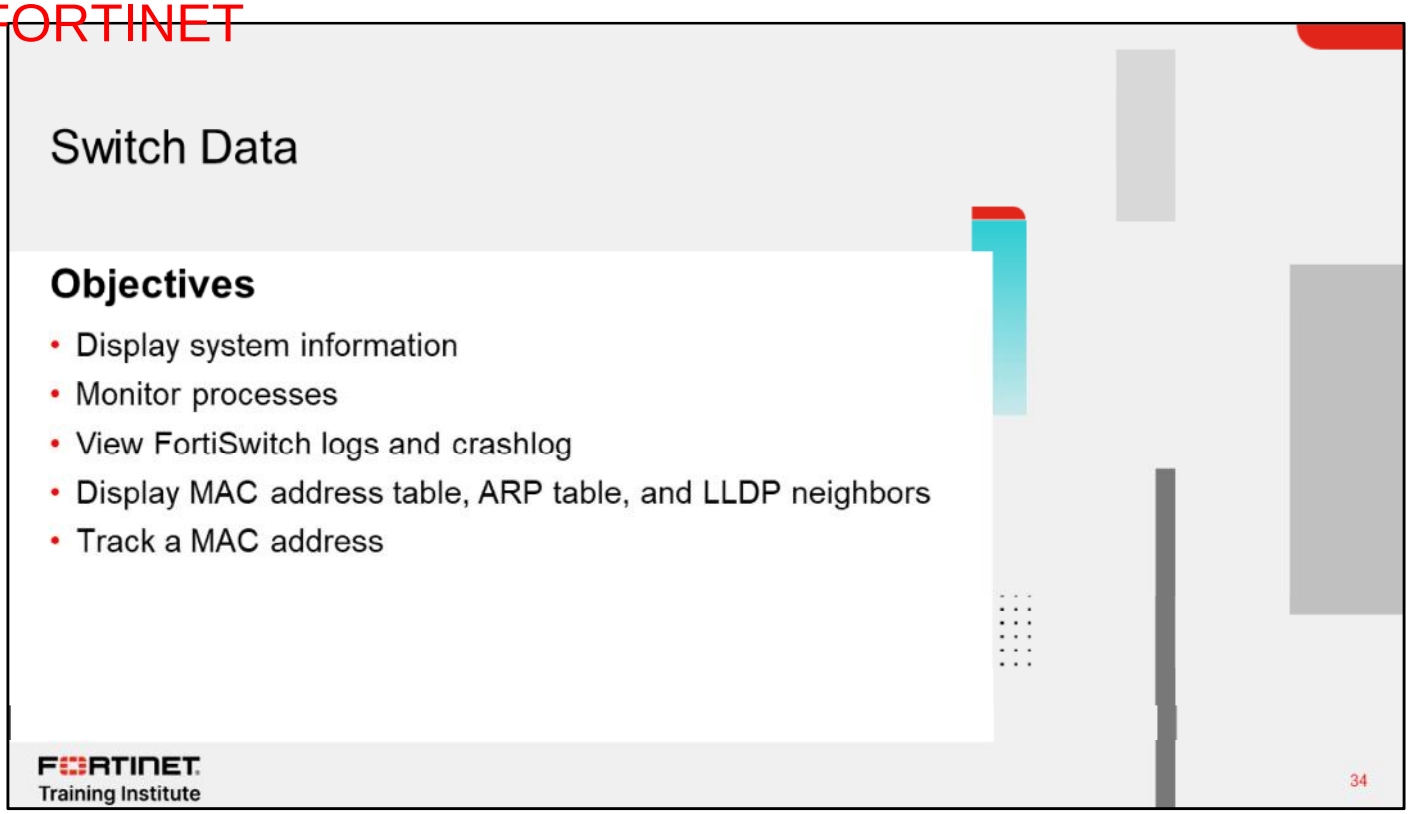


Good job! You now understand how to troubleshoot switch interfaces.

Now, you will learn about gathering important switch data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

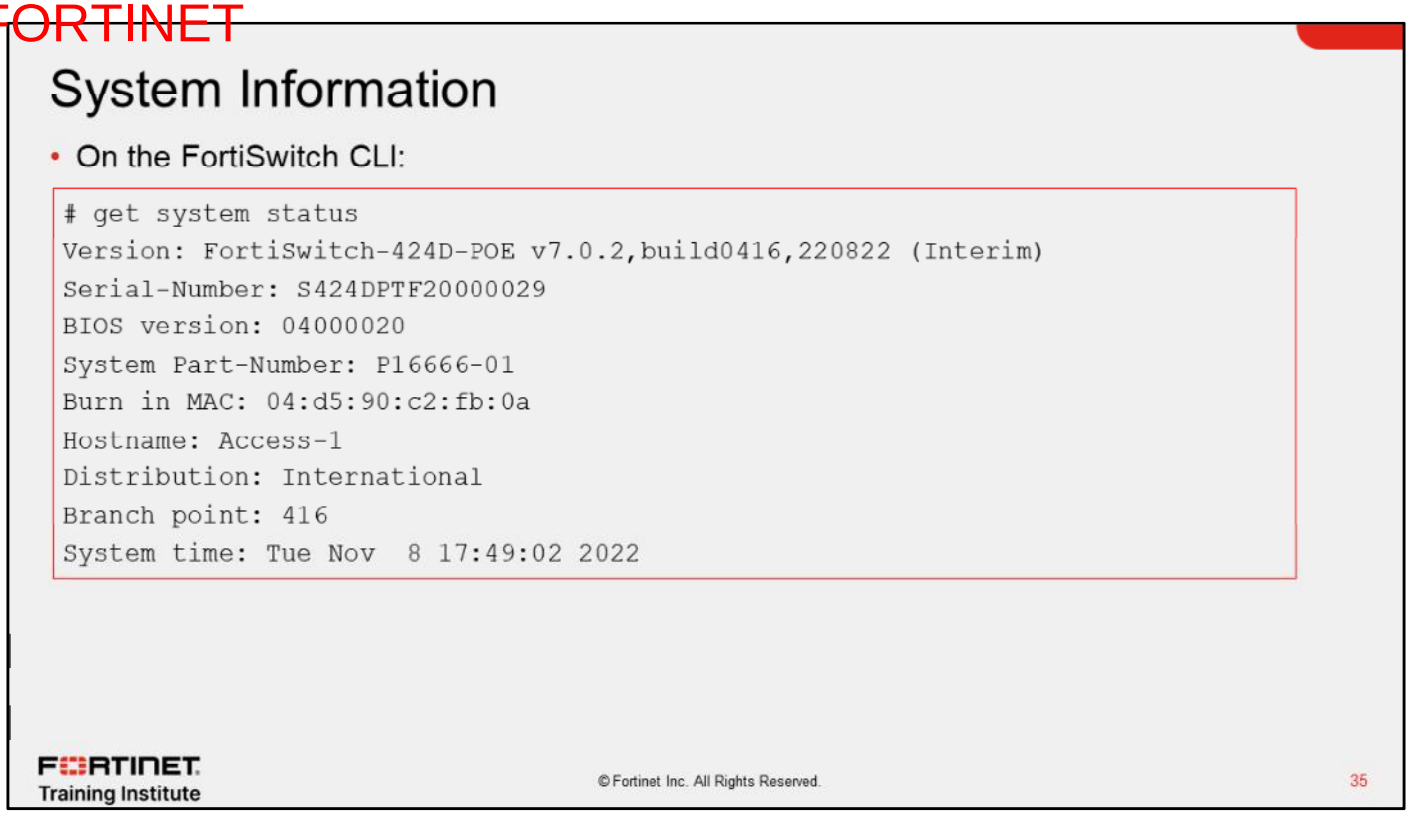


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in gathering switch data, you should be able to collect important diagnostic information on FortiSwitch for troubleshooting purposes.

Vouchers & Dumps are Available | WhatsApp +201224560923

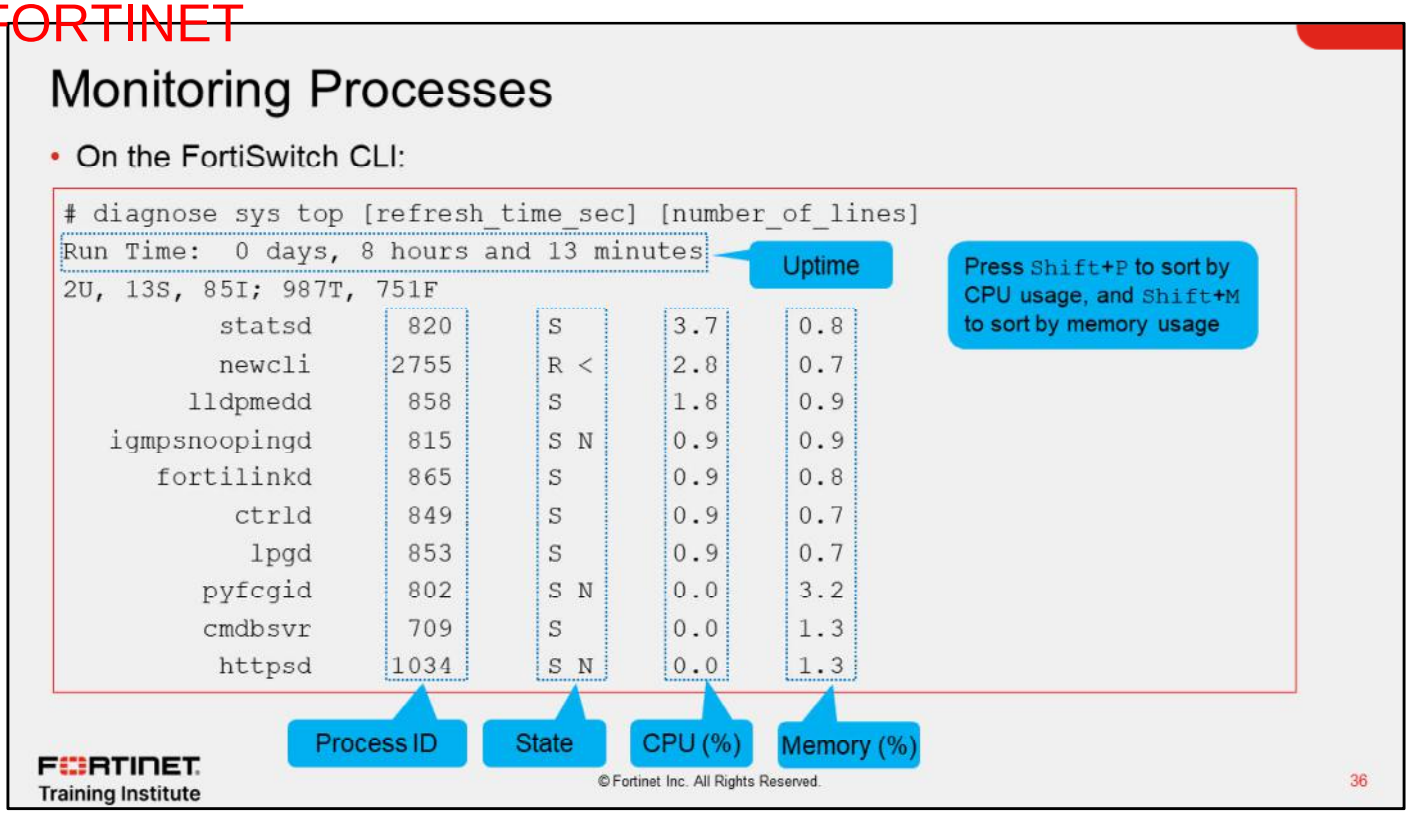
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The command shown on this slide is usually one of the first debug commands that you use on FortiSwitch when troubleshooting. The output shows the following information about the switch: firmware version, serial number, main MAC address, and time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows you how to display the amount of CPU and memory (in percentage) in use by each process. The command shown on this slide displays the information shown in the last column. For each process, the command also displays the ID number and state. You can specify the refresh frequency and the number of lines to display.

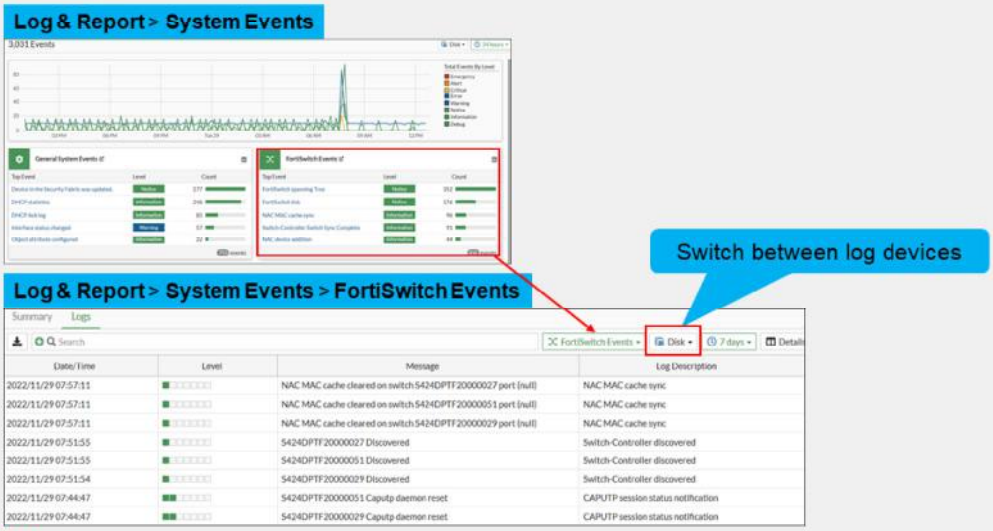
While the command is running, you can press `Shift+P` to sort the processes by CPU use, or `Shift+M` to sort them by memory use. To stop the command, press `q` or `Q`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSwitch Logs—FortiGate GUI

- FortiSwitch logs are displayed on the FortiGate GUI as events logs in a separate sub-category



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

This slide shows an example of some FortiSwitch logs displayed on the FortiGate GUI. FortiSwitch logs are available as events logs on the FortiGate GUI, under the **FortiSwitch Events** sub-category.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Logs—FortiGate CLI

- Set filter to event logs (category `1`) and `subtype` to `switch-controller` before displaying the logs on the CLI

```
# execute log filter category 1
# execute log filter field subtype switch-controller
# execute log display
48 logs found.
10 logs returned.

1: date=2020-12-08 time=09:51:10 eventtime=1607449870305048995 tz="-0800" logid="0114032602"
type="event" subtype="switch-controller" level="information" vd="root" logdesc="Switch-Controller
authorized" user="admin" ui="GUI(10.0.1.10)" sn="S224EPTF19005928" name="S224EPTF19005928"
msg="S224EPTF19005928 Authorized"

2: date=2020-12-08 time=09:47:26 eventtime=1607449646914451629 tz="-0800" logid="0114032601"
type="event" subtype="switch-controller" level="information" vd="root" logdesc="Switch-Controller
discovered" user="Switch-Controller" ui="fortilinkd" sn="S224EPTF19005928" name="S224EPTF19005928"
msg="S224EPTF19005928 Discovered"
...
```

FORTINET Training Institute

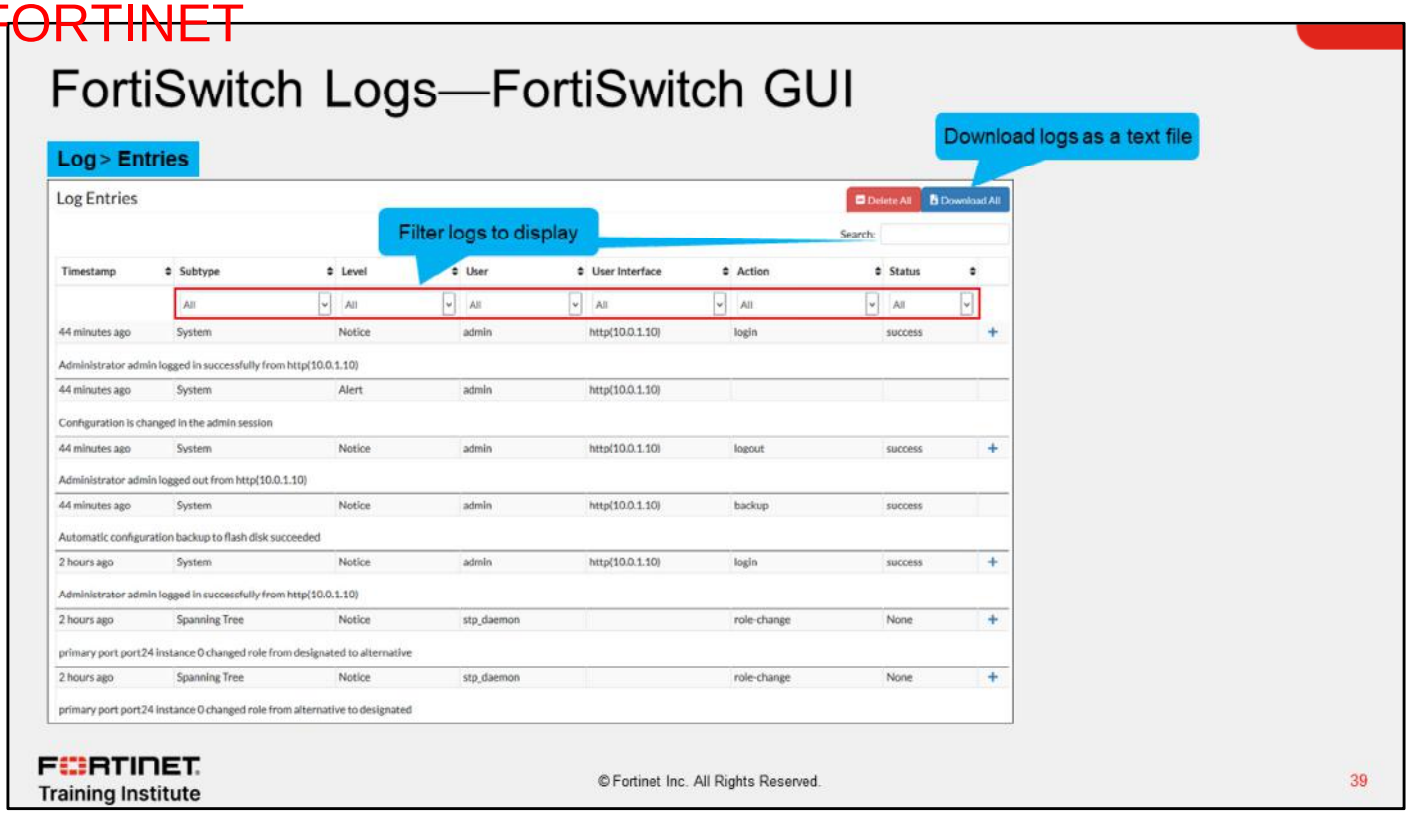
© Fortinet Inc. All Rights Reserved.

38

You can also display the FortiSwitch logs on the FortiGate CLI. Just set the filter to event logs (category `1`) and `subtype` to `switch-controller`. The example on this slide shows how to set up the filter and display the logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

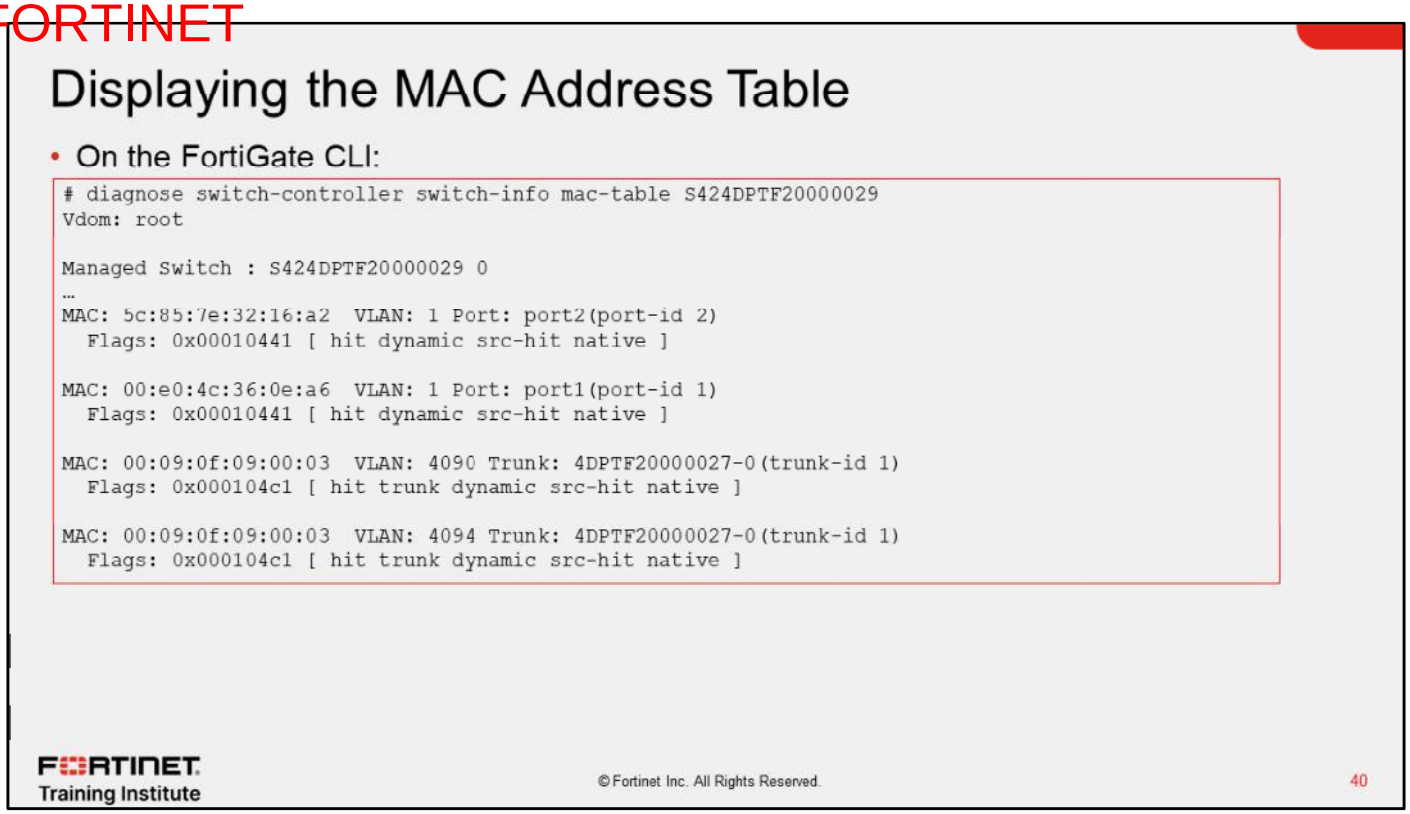
DO NOT REPRINT
© FORTINET
Brave-dumps.com



On the FortiSwitch GUI, browse to the **Log** page to display the local logs generated by the system. Here, you can download the logs as a text file or delete them. There are also a filter toolbar and a search bar that you can use to display specific logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On FortiGate, the command `diagnose switch-controller switch-info mac-table` displays the FortiSwitch MAC address table. The default aging timer for learned MAC addresses is 300 seconds (5 minutes).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying the MAC Address Table (Contd)

- To display the MAC address table on the FortiSwitch CLI:

```
# diagnose switch mac-address list

MAC: 00:50:56:96:d8:02  VLAN: 4094 Trunk: _FlInK1_MLAG0_(trunk-id 1)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 00:e0:4c:36:0e:a6  VLAN: 10 Port: port1(port-id 1)
  Flags: 0x00010441 [ hit dynamic src-hit native ]
...

Total Displayed: 17
```

- Adjust the filter to display the entries on a given port only:

```
# diagnose switch mac-address filter port-id-map 1

# diagnose switch mac-address list

MAC: 00:e0:4c:36:0e:a6  VLAN: 10 Port: port1(port-id 1)
  Flags: 0x00010441 [ hit dynamic src-hit native ]

Total Displayed: 1
```

port1

FORTINET Training Institute

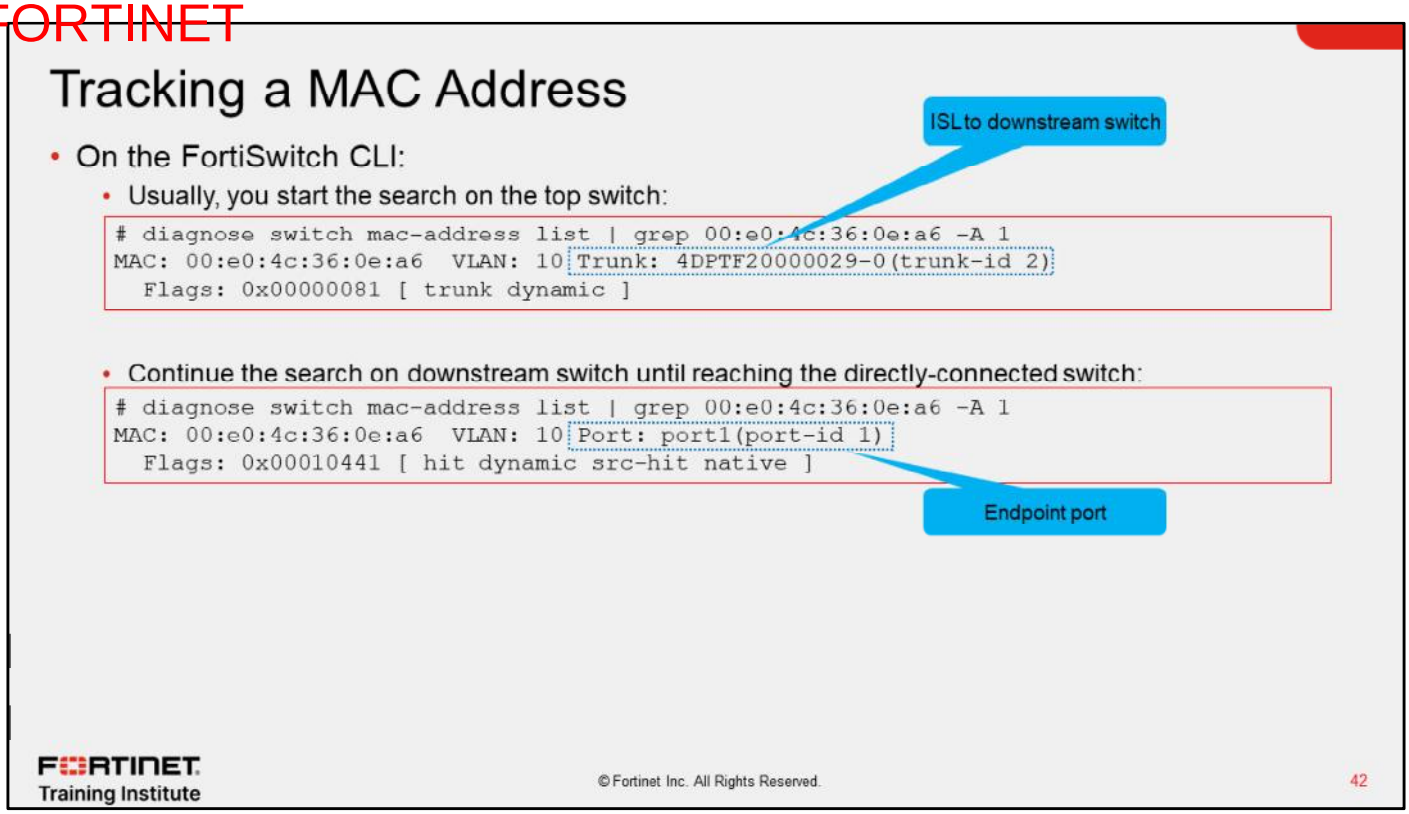
© Fortinet Inc. All Rights Reserved.

41

On FortiSwitch, you can use the `diagnose switch trunk list` command to display the FortiSwitch MAC address table. Set up the command filter, as shown on this slide, to display the entries on a given port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

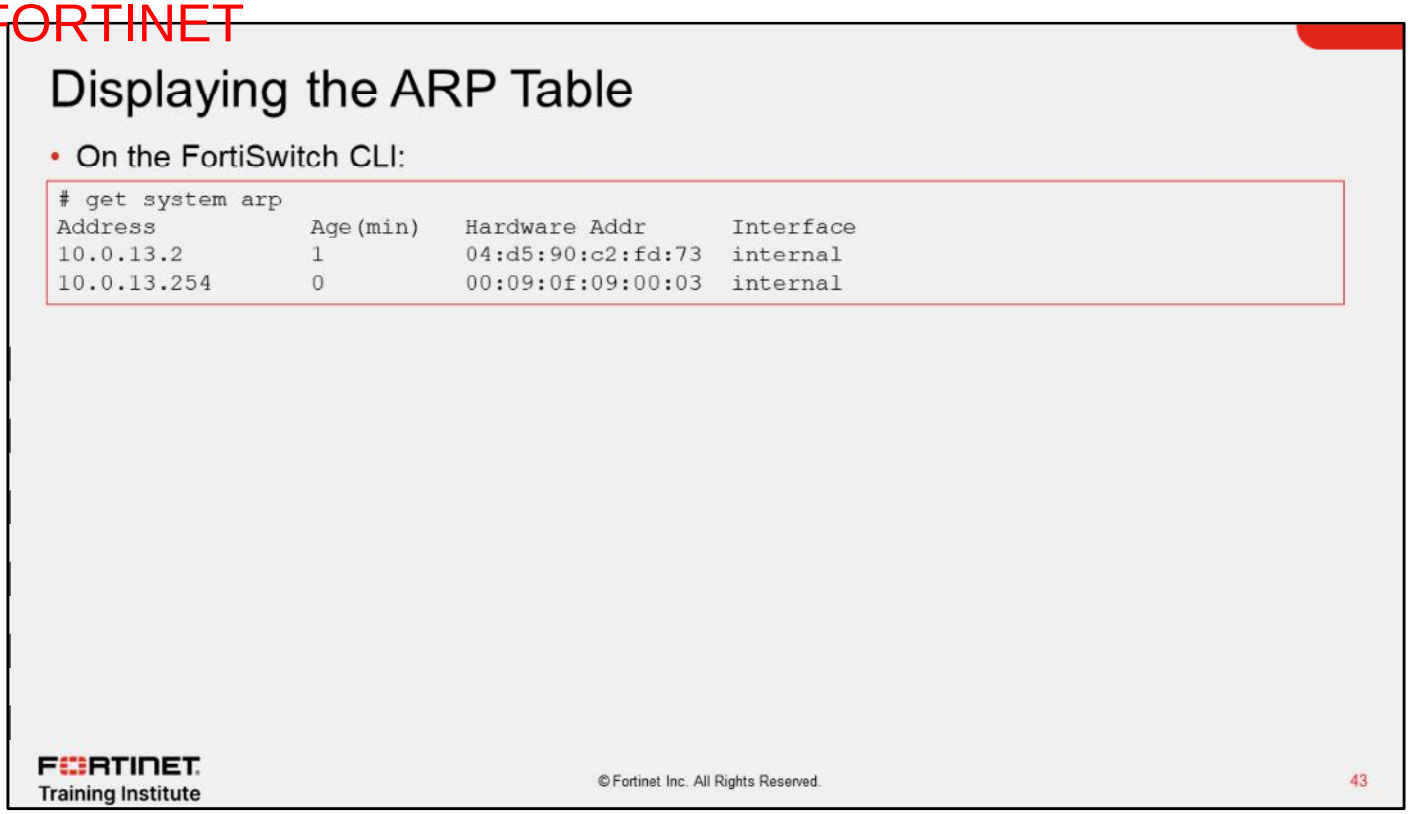


Sometimes you need to locate a device by MAC address. For this, you can use the `diagnose switch mac-address list` command, and then grep the output with the MAC address to look up, as shown on this slide.

You usually start the search on the top switch of your stack. You identify the downstream switch by the port or trunk shown on the MAC address table search results. You then continue moving down the switch stack until reaching the switch that connects directly to the device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Like any other IP device, FortiSwitch maintains an ARP table that contains entries for IP addresses and their corresponding MAC address. Usually, you want to check the ARP table if you face issues when FortiSwitch terminates or initiates the connection, such as issues with management traffic and remote server authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying LLDP Neighbors—Summary

- On the FortiGate CLI:

```
# diagnose switch-controller switch-info lldp neighbors-summary S548DF4K16000693
Vdom: root
Managed Switch : S548DF4K16000693       0

Capability codes:
        R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device
        W:WLAN Access Point, P:Repeater, S:Station, O:Other
MED type codes:
        Generic:Generic Endpoint (Class 1), Media:Media Endpoint (Class 2)
        Comms:Communications Endpoint (Class 3), Network:Network Connectivity Device

  Portname    Status   Device-name                TTL   Capability  MED-type  Port-ID
  _________   _______  _________________________  ____  __________  ________  _______
  port1       Up       -                          -     -           -         -
  port2       Up       -                          -     -           -         -
...
  port51      Up       FG-601E-Active             120   BR          -         04:d5:90:dc:35:34
  port52      Up       FG-601E-Backup             120   BR          -         04:d5:90:dc:07:7c
  port53.1    Up       426ef                      120   BR          -         port27
...
```

FortiGate port MAC address

- Equivalent command on the FortiSwitch CLI:

```
# get switch lldp neighbors-summary
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

On FortiGate, you can use the FortiGate CLI to display the LLDP neighbors discovered by your stack of switches. This slide shows the command you can run to display a summary of the information learned from LLDP on each port. Usually, you are interested in looking at the `Device-name` and `Port-ID` columns, which enables you to quickly identify the adjacent neighbor and port. On FortiSwitch, you can obtain the same output by running the command shown on this slide.

Note that in the example, FortiGate advertises the MAC address of its port as the port ID. This happens when the FortiGate port does not have an alias configured. If an alias is set, FortiGate then advertises the alias as the port ID instead.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Displaying LLDP Neighbors—Detail

- On the FortiGate CLI:

```
# diagnose switch-controller switch-info lldp neighbors-detail port24
Vdom: root
Managed Switch : S224EPTF19005928       0

Capability codes:
        R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device
        W:WLAN Access Point, P:Repeater, S:Station, O:Other

MED TLV Capability codes:
        C:Capabilities, P:Network Policies, L:Location, S:MDI PSE
        D:MDI PD, I:Inventory

_____________________________________________________________
Neighbor learned on port port24 by LLDP protocol
Last change 23 seconds ago
Last packet received 0 seconds ago

Chassis ID: 00:50:56:96:f8:43 (mac)
System Name: FortiGate.trainingAD.training.lab
System Description:
FortiGate-VM64 v7.2.1,build1254,220803 (GA.F)
...
```

FortiOS version

FORTINET Training Institute

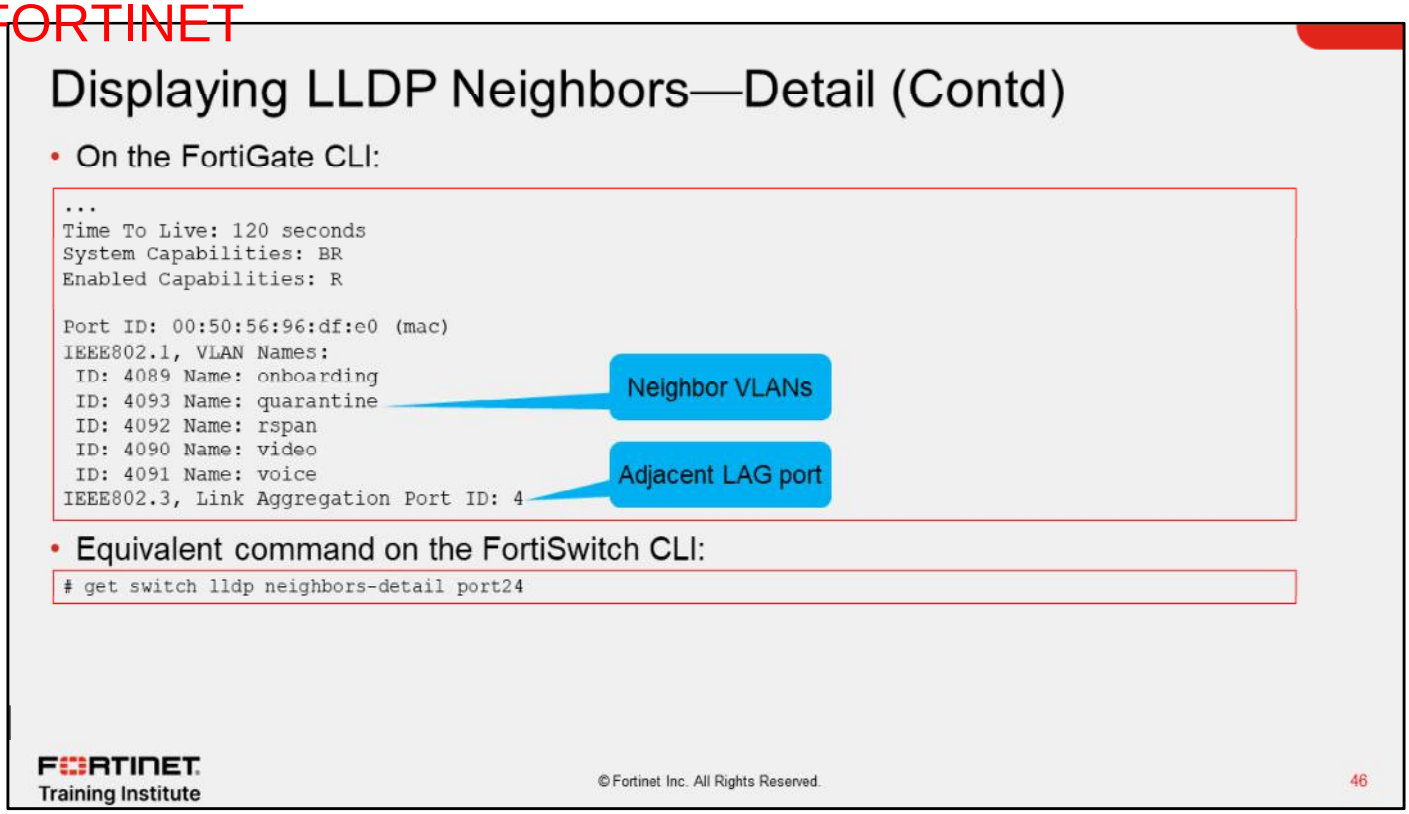
© Fortinet Inc. All Rights Reserved.

45

On FortiGate, use the command shown on this slide to display all the information learned from LLDP on a specific port. The output was cropped to fit the slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

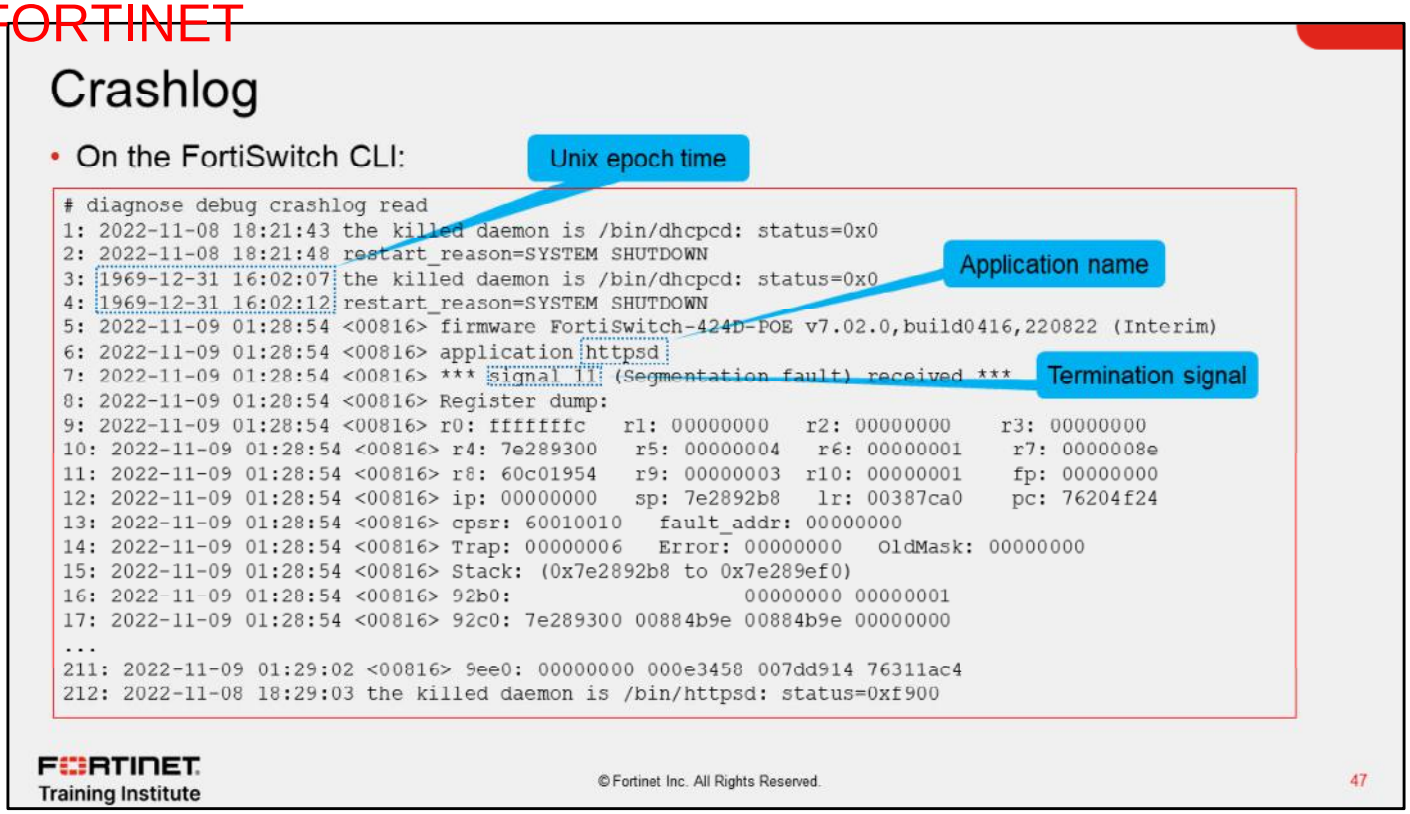


This slide shows the remaining portion of the LLDP detailed output. Note that the VLANs present in the neighbor are also included in the output. In addition, because the neighbor is connected over a trunk, the output also indicates the port ID (port4) of the port on the adjacent device used for the LAG. On FortiSwitch, you can obtain the same output by running the command shown on this slide.

Note that the information displayed for each neighbor depends on the information it advertises. Therefore, expect the information to vary across different device types and vendors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



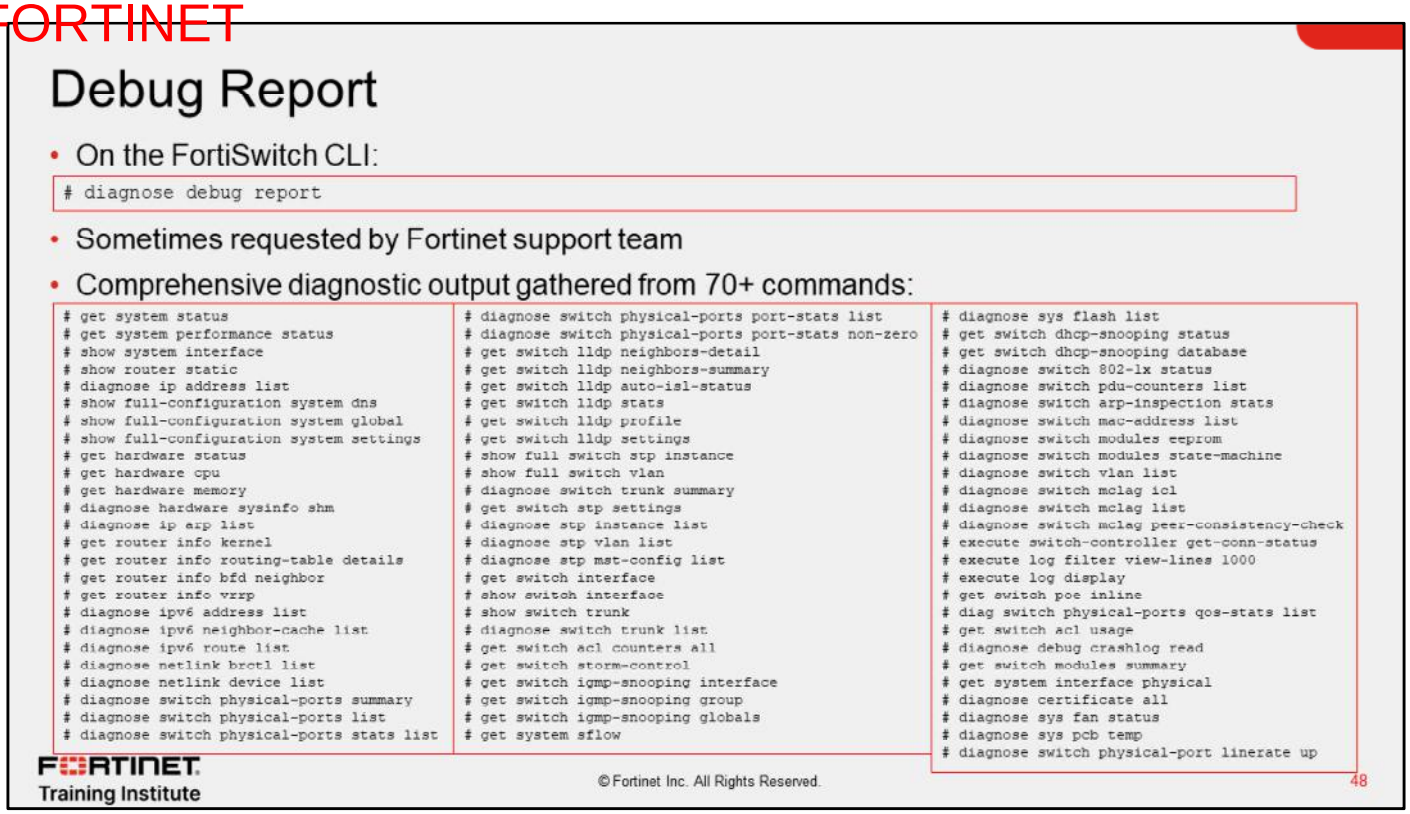
Each time an application crashes or closes, an entry is generated in the crashlog. When an application crashes, the entry contains the name of the application, the time it crashed, and the termination signal.

This slide shows a sample of a crash in the crashlog. In this example, the application that failed was the `httpsd` process, which handles the GUI and REST API interfaces. The termination signal is `11`, which is a segmentation fault.

Note that the crashlog shows the Unix epoch time as timestamps for two messages. This is because the messages were generated before the switch synchronized its time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can run the `diagnose debug report` command on the FortiSwitch CLI to generate a comprehensive diagnostic output that is gathered from the execution of more than 70 CLI commands, which are shown on this slide.

The output of `diagnose debug report` is sometimes requested by Fortinet Technical Support, if an exhaustive analysis of the device is required, or just to ensure that further information is collected ahead of time, in case it is needed later on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiSwitchOS command displays the switch uptime?

A. `get system status`
✓ B. `diagnose sys top`

2. Which FortiSwitchOS command displays the switch MAC address table?

✓ A. `diagnose switch mac-address list`
B. `diagnose switch-controller switch-info mac-table`

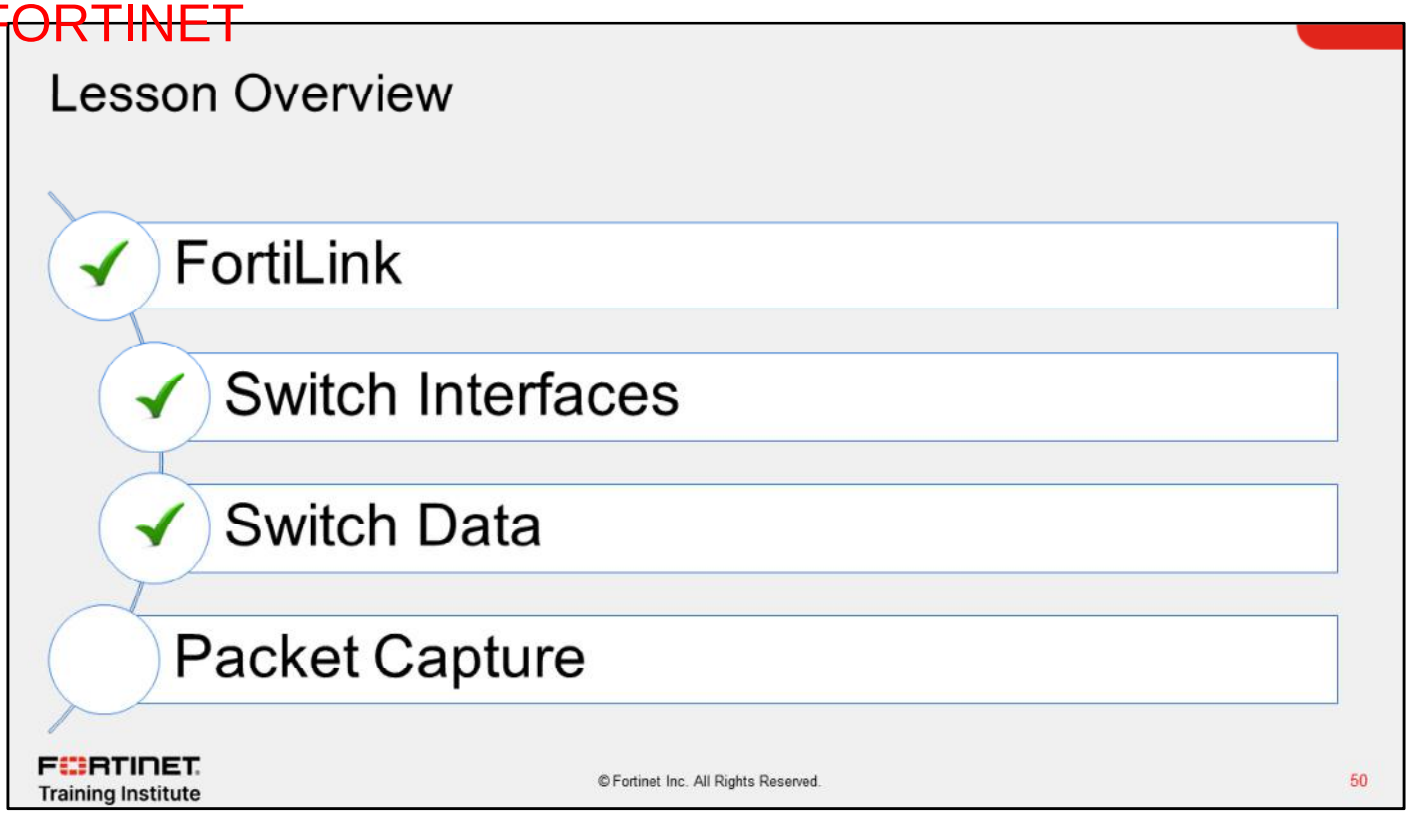
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

49

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

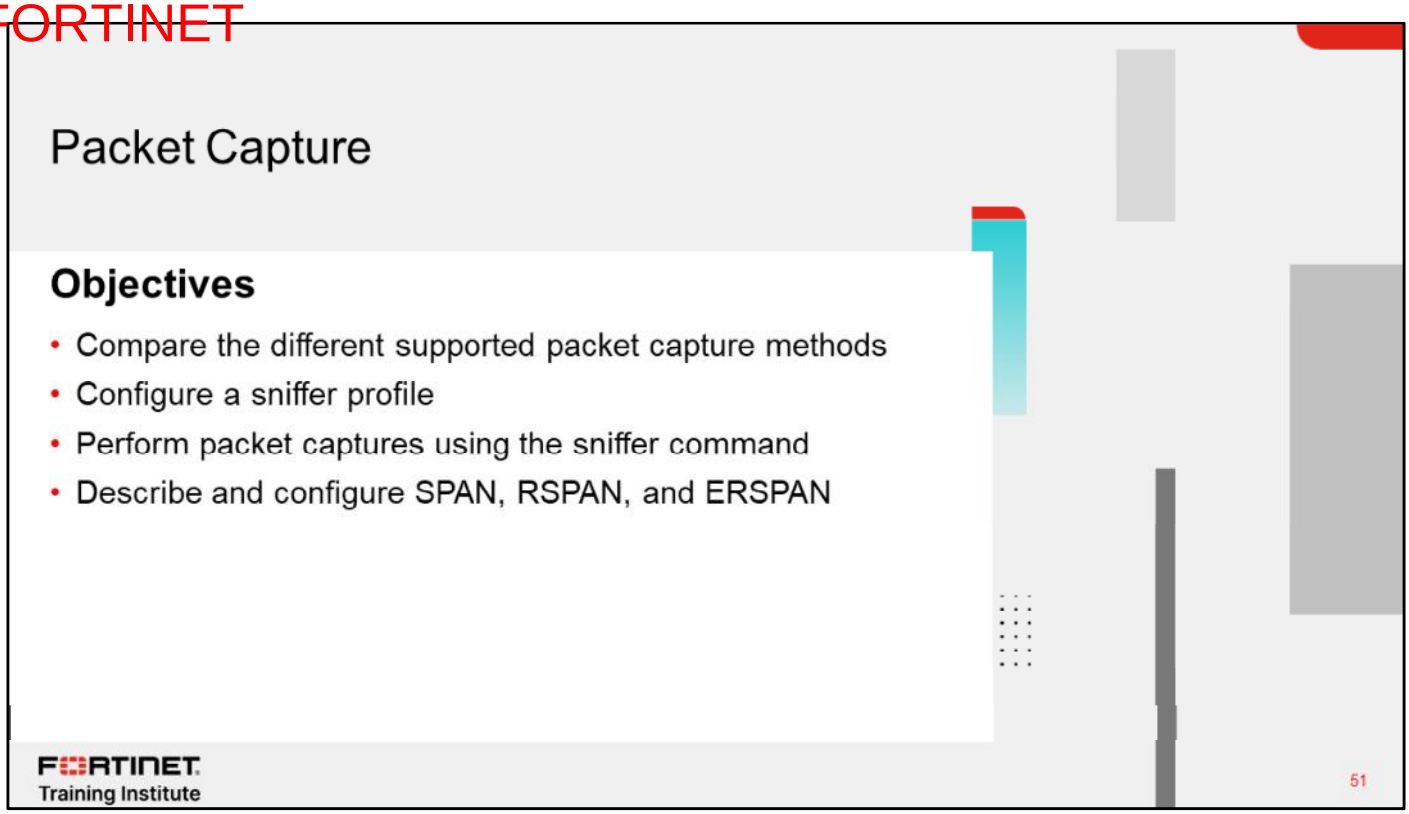


Good job! You now understand how to gather switch data.

Now, you will learn about the different packet capture methods available on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in packet capture, you should be able to identify the most useful packet capture method for your troubleshooting session.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Choosing a Packet Capture Method

Method	Can be configured on		Supported Capturing Interfaces					Remarks
	FortiGate	FortiSwitch	internal	mgmt	Switch ports	Trunks	Multiple	
Sniffer Profile		GUI, CLI	X	X	X	X	X*	Traffic captured on trunks may not include egress management traffic
Sniffer Command		CLI	X	X	X		X*	Traffic captured on switch ports is limited to only ingress Layer 2 traffic such as LLDP and STP
SPAN	CLI	GUI, CLI			X	X	X	
RSPAN	CLI	GUI, CLI			X		X	In managed switch mode, mirrored traffic is always forwarded to FortiGate
ERSPAN	CLI	GUI, CLI			X		X	In managed switch mode, ERSPAN collector IP can't be in the FortiLink interface subnet
sFlow	CLI	GUI, CLI	X**		X	X	X	Set sampling rate to 1 to capture all packets

* You must configure multiple sniffer profiles, or run multiple sniffer commands

** Supported on only the FortiSwitch GUI and the FortiSwitch CLI

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

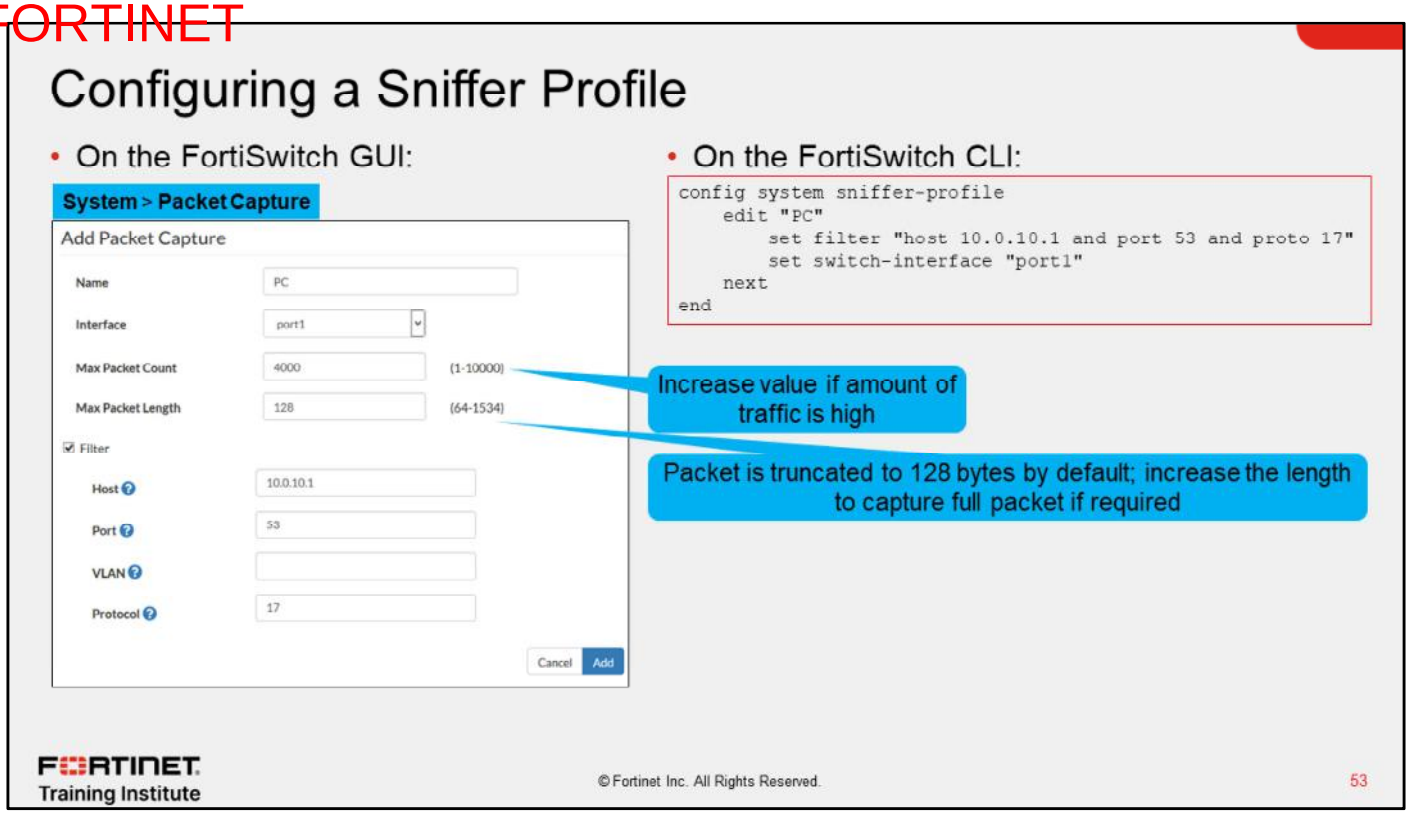
52

There are plenty of packet capture methods to choose from on FortiSwitch. The chosen method depends on the FortiSwitch management mode, the interface type you want to capture traffic on, the type of the traffic you plan to capture, and how you plan to collect the captured traffic.

The table shown on this slide compares the six methods available and their supported features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

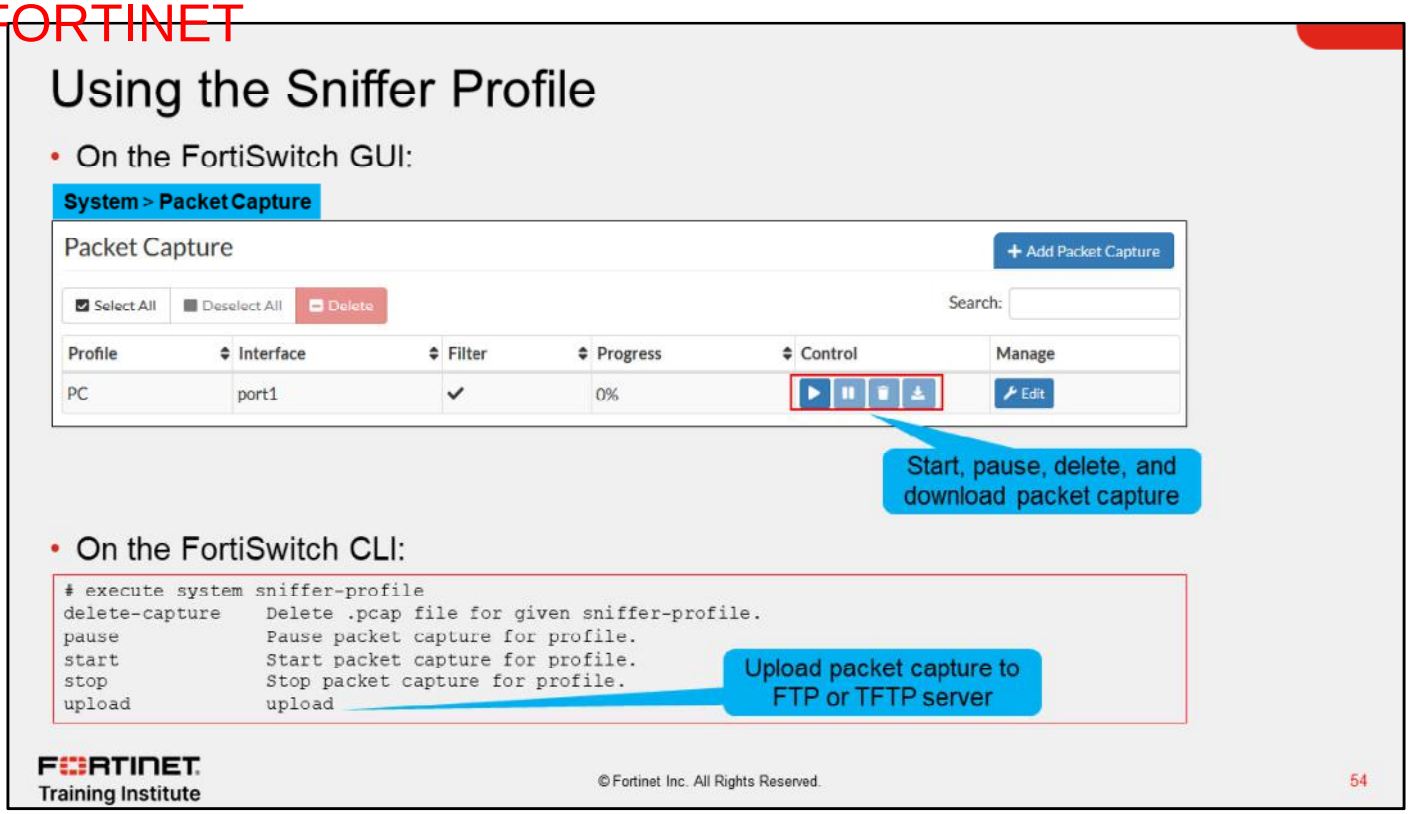


This slide shows an example of a basic sniffer profile configuration using the FortiSwitch GUI and CLI. Note that you must specify the maximum number of packets on the capture. For this reason, keep in mind that not all the packets may be captured if the amount of traffic is excessive.

Also note that, by default, FortiSwitch truncates the captured packet to a length of 128 bytes. Usually, this is not a problem in most troubleshooting cases. However, you can increase the maximum packet length if you need to capture the complete packet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you configure the sniffer profile, you can start, pause, delete, or download the packet capture by using the control buttons highlighted on the screenshot on this slide. Alternatively, you can use the FortiSwitch CLI as shown on this slide. Usually, it is more convenient to use the FortiSwitch GUI because you can download the packet capture from the **Packet Capture** page. If you use the FortiSwitch CLI, you must upload the packet capture to an FTP or TFTP server, which can sometimes delay the troubleshooting process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Using the Sniffer Command on the FortiSwitch CLI

```
# diagnose sniffer packet <interface> '<filter>' <level> <count> <tsformat>
```

<count> stops packet capture after this many packets

<tsformat> changes the time stamp format:

a – Absolute UTC time

Level	IP headers	IP payload	Ethernet headers	Port names
1	✓			
2	✓	✓		
3	✓	✓	✓	
4	✓			✓
5	✓	✓		✓
6	✓	✓	✓	✓

FORTINET Training Institute

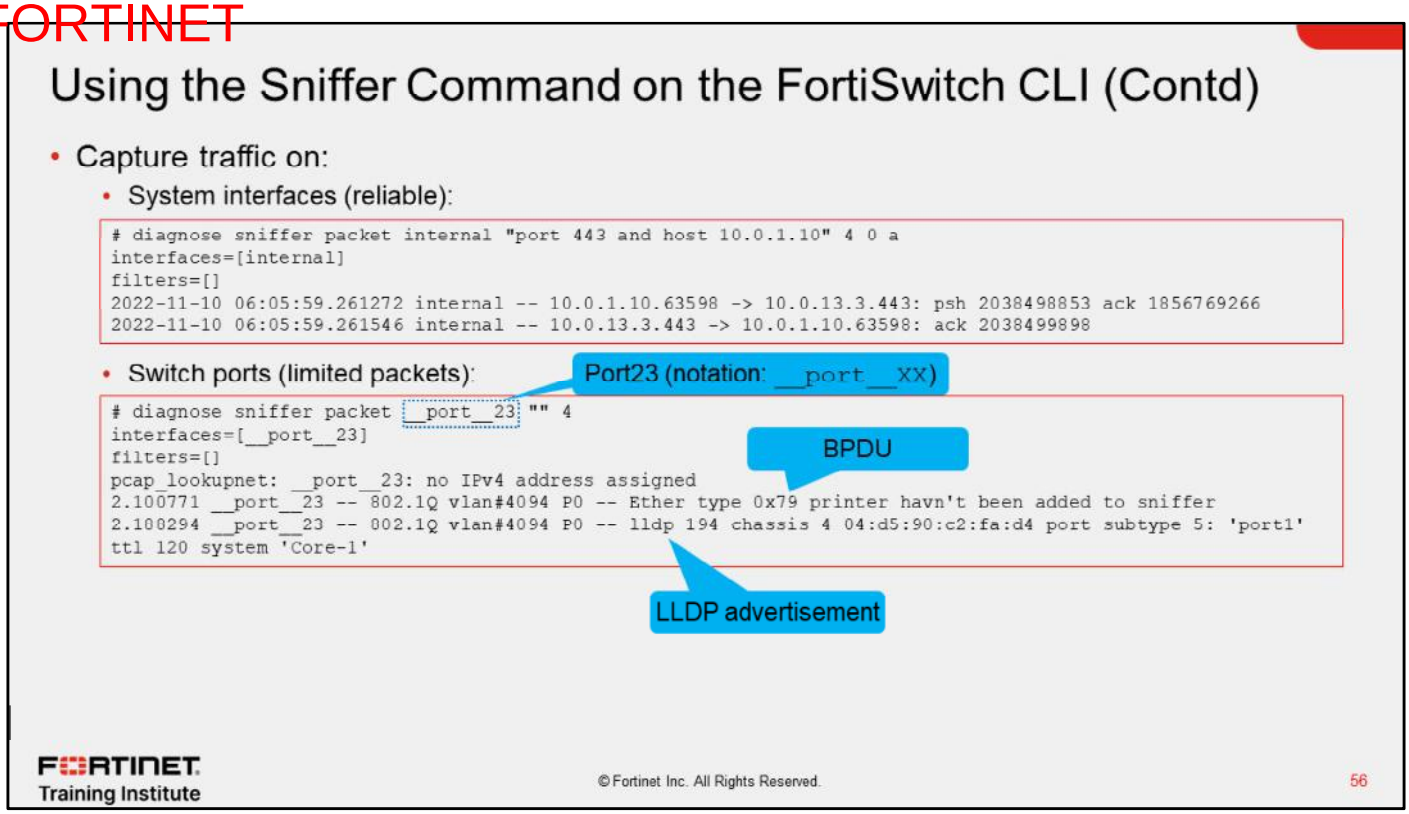
© Fortinet Inc. All Rights Reserved.

55

If you are familiar with the FortiGate sniffer command, then you also know how to use the sniffer command on FortiSwitch. Like FortiGate, you can choose from six verbosity levels. The table on this slide shows what information is displayed in each level. Level 4 is preferred in most of the cases, because it displays a summary of the packet and the interface the packet leaves or enters. Level 3 or Level 6 can be used to convert the output to PCAP format, which can later be examined with a network protocol analyzer, such as Wireshark.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows how to capture traffic on system interfaces and switch ports.

If you want the packet capture to be reliable, then avoid using the sniffer command to capture traffic on interfaces other than system interfaces, such as `internal` and `mgmt`. Although you can also use the sniffer command to capture traffic on switch ports, as shown on this slide, the types of packets captured by the sniffer are very limited. In the example shown on this slide, the sniffer displays only ingress LLDP advertisements and BPDUs when capturing traffic on port23, even though, at the time of the capture, there was more traffic being sent and received on the port.

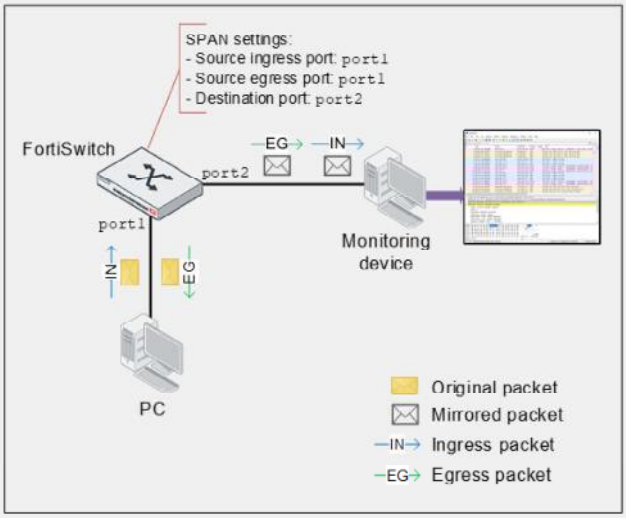
Note the use of the notation `__port__XX` to reference a switch port in the sniffer command.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is SPAN?

- Mirrors traffic on a port to selected destination interface
  - Both ingress and egress traffic can be mirrored
  - No encapsulation
  - Mirrored port must be a switch port
  - All traffic is mirrored
  - Filtering options available when combined with ACL
    - Only in standalone mode
- Limitations
  - Mirrored traffic can't span multiple switches
  - No support for system interfaces
  - No filtering options in managed switch mode



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

57

Switch port analyzer (SPAN) enables you to mirror traffic on one or more ports to the specified destination interface, where a monitoring device, such as a PC running Wireshark, is connected and capturing the mirrored traffic.

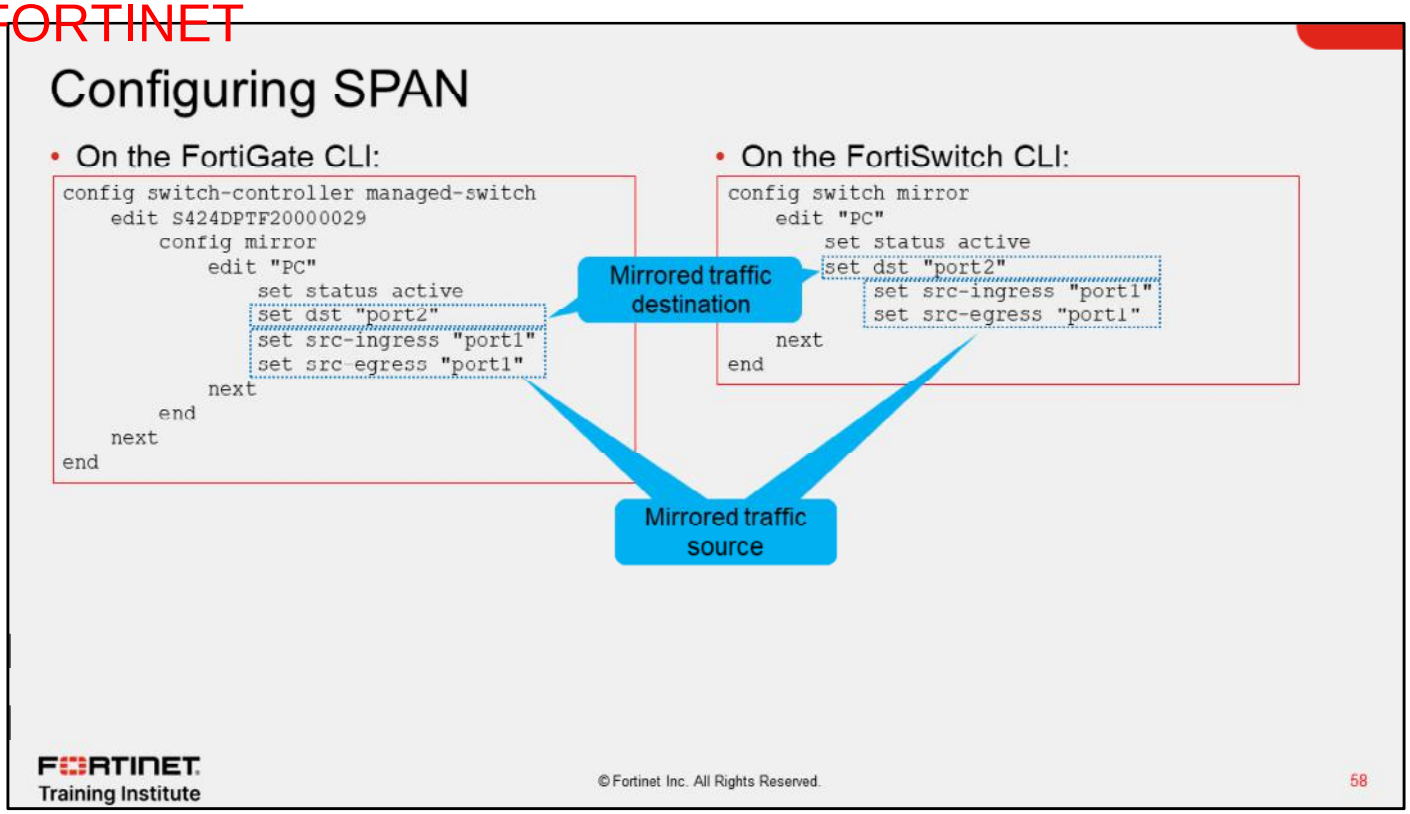
When you configure SPAN, you can configure FortiSwitch to mirror ingress or egress traffic on the port. Also, because FortiSwitch does not encapsulate the mirrored traffic, the traffic captured on the monitoring device is an exact copy of the original.

Unlike remote SPAN (RSPAN) and encapsulated remote SPAN (ERSPAN), you can't send the mirrored traffic across multiple switches when you use SPAN. For this reason, the monitoring device must be connected to the same switch where the traffic is being mirrored. Another limitation of using SPAN is that you can mirror traffic on switch ports only. That is, traffic on system interfaces, such as internal or mgmt can't be mirrored. In addition, SPAN mirrors all the traffic on a port. However, if FortiSwitch is in standalone mode, you can filter the traffic to capture by configuring an ACL classifier and referencing the SPAN profile.

In the example shown on this slide, SPAN is enabled on FortiSwitch, and is configured to mirror ingress and egress traffic on port1, to port2. As a result, ingress and egress traffic generated by the PC can be captured on the monitoring device using Wireshark.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



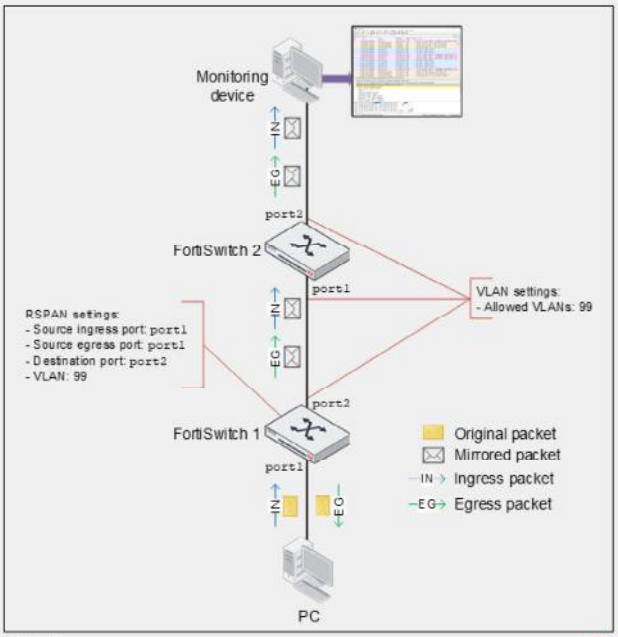
This slide shows an example of how to configure a basic SPAN session on the FortiGate CLI and on the FortiSwitch CLI. The settings instruct FortiSwitch to mirror the ingress and egress traffic on port1, to port2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is RSPAN?

- Mirrors traffic on a port to a destination port and VLAN:
  - Both ingress and egress traffic can be mirrored
  - Mirrored traffic:
    - Is tagged with configured VLAN and *flooded*
      - Best practice: use a dedicated VLAN for RSPAN
      - In managed switch mode, mirrored traffic is tagged with the rspan VLAN and forwarded to FortiGate only
    - Can span multiple switches that accept the VLAN
  - Mirrored port must be a switch port
  - All traffic is mirrored
  - Filtering options available when combined with ACL
    - Available in both managed switch and standalone modes
- Limitations
  - Mirrored traffic can't span Layer 3 devices
  - No support for system interfaces



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

59

RSPAN is an enhanced version of SPAN. Like SPAN, it enables you to mirror traffic on one or more ports to the specified destination interface. However, unlike SPAN, RSPAN tags the mirrored traffic with a VLAN of your choice, and then floods the traffic in the VLAN across multiple switches. The result is that all devices in the VLAN receive a copy of the mirrored traffic. For this reason, to prevent network saturation caused by the mirrored traffic, it is a common best practice to use a dedicated VLAN for RSPAN, and to assign to the VLAN the monitoring devices only.

Note that in managed switch mode, FortiSwitch uses the **rspan** VLAN (VLAN ID 4092) as the destination VLAN for mirrored traffic. In addition, the mirrored traffic is forwarded across the stack only to ports leading to FortiGate, thus preventing traffic flood. Then, on FortiGate, you must use the sniffer to capture the mirrored traffic.

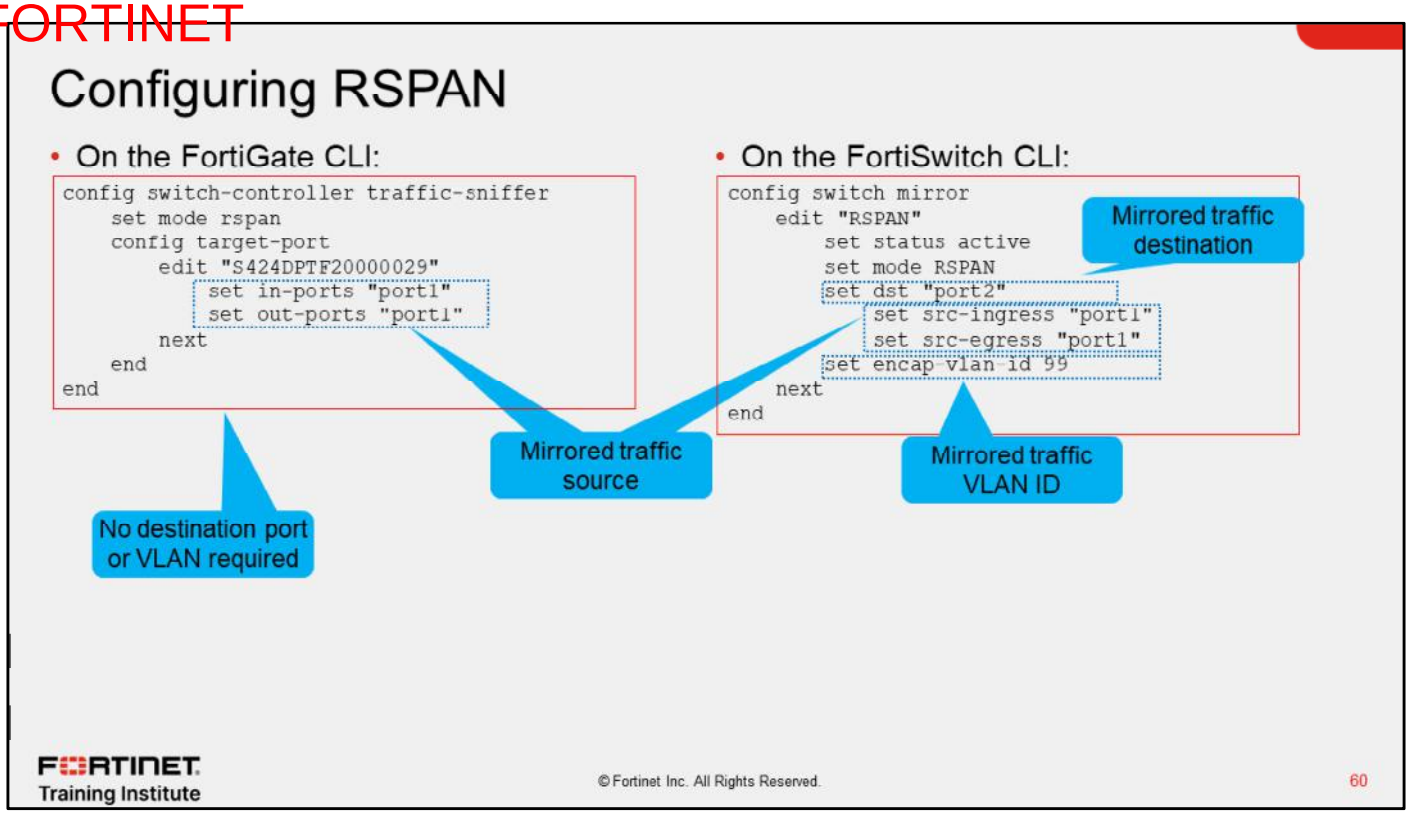
Like SPAN, RSPAN mirrors all the traffic on a port. However, you can filter the traffic to capture—regardless of the FortiSwitch management mode—by configuring an ACL classifier and referencing the SPAN profile.

Unlike ERSPAN, RSPAN can't send mirrored traffic across multiple Layer 3 devices, such as routers and firewalls. For this reason, the monitoring device must be connected to the same Layer 2 domain where the traffic is being mirrored.

The example shown on this slide describes RSPAN operation when *FortiSwitch is in standalone mode*. RSPAN is enabled on FortiSwitch 1, and is configured to mirror ingress and egress traffic on port1. The mirrored traffic is flooded to port2 and tagged with VLAN 99. The ports used in the ISL, as well as port2 on FortiSwitch 2, allow VLAN 99. As a result, ingress and egress traffic generated by the PC can be captured on the monitoring device using Wireshark.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows an example of how to configure a basic RSPAN session on the FortiGate CLI and FortiSwitch CLI. The settings instruct FortiSwitch to mirror the ingress and egress traffic on port1, to port2, and tag the mirrored traffic with VLAN ID 99.

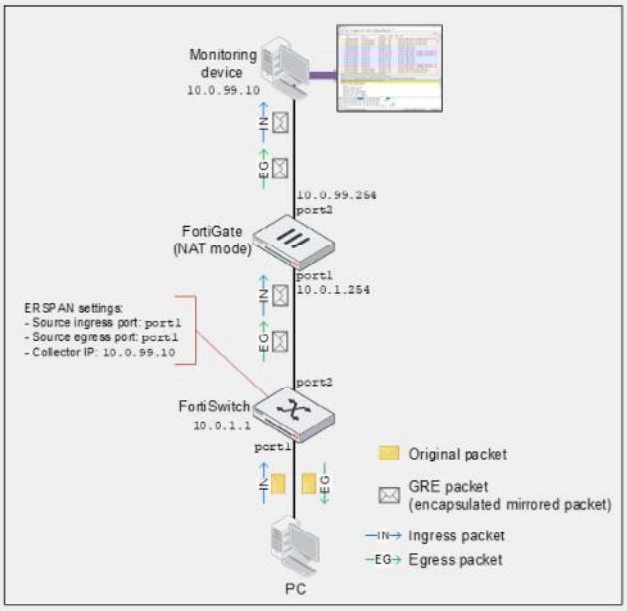
Note that when you use the FortiGate CLI to configure RSPAN, you don't indicate the destination port or the VLAN ID. This is because FortiGate automatically configures FortiSwitch to forward mirrored traffic to ports leading to FortiGate, and tags the traffic with VLAN ID 4092, which is the VLAN ID assigned to the **rspan** VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is ERSPAN?

- Mirrors traffic on a port to a collector IP
  - Both ingress and egress traffic can be mirrored
  - Mirrored traffic:
    - Is encapsulated in GRE
    - Can span multiple Layer 3 devices
  - Mirrored port must be a switch port
  - All traffic is mirrored
  - Filtering options available when combined with ACL
    - Available in both managed switch and standalone modes
- Limitations
  - ERSPAN collector IP can't be in the FortiLink interface subnet
  - No support for system interfaces



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

61

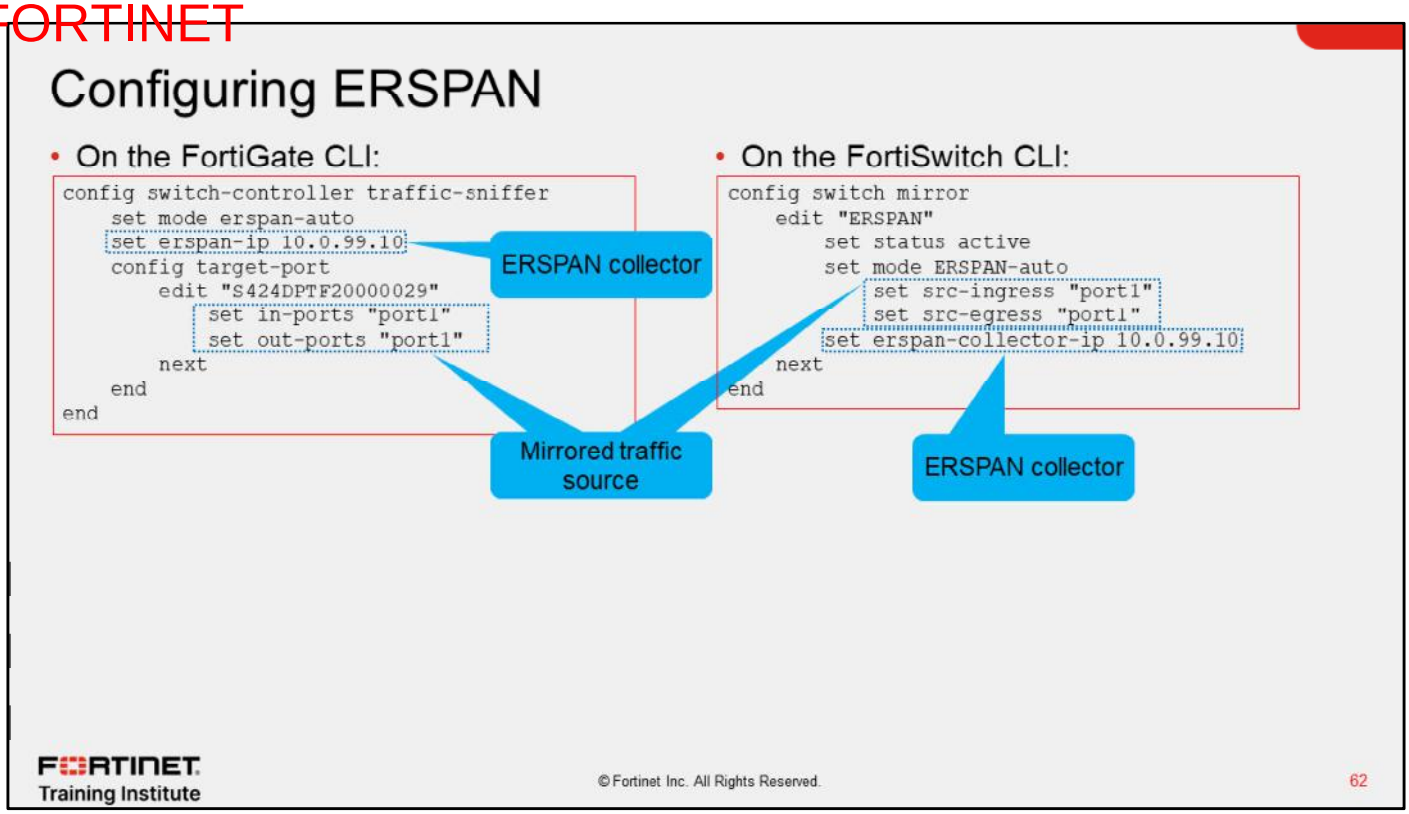
ERSPAN enables you to send the mirrored traffic across multiple Layer 3 devices. For this, ERSPAN encapsulates the mirrored traffic into GRE packets, and sends the packets to the configured collector IP. This enables you to use any collector in your network, as long as FortiSwitch has IP connectivity with that device.

Note that if you are using FortiSwitch in managed switch mode, the collector IP can't be in the same subnet as your FortiLink interface.

In the example shown on this slide, ERSPAN is enabled on FortiSwitch, and is configured to mirror ingress and egress traffic on port1. The mirrored traffic is encapsulated into GRE packets, and sent to `10.0.99.10`, which is the IP address of the monitoring device connected behind FortiGate. FortiGate receives the GRE packets on port1, and routes them to port2. As a result, ingress and egress traffic generated by the PC can be captured on the monitoring device using Wireshark.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows an example of how to configure a basic ERSPAN session on the FortiGate CLI and on the FortiSwitch CLI. The settings instruct FortiSwitch to mirror the ingress and egress traffic on port1, and send the GRE packets carrying the mirrored traffic to `10.0.99.10`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which traffic mirroring method enables you to send mirrored traffic across Layer 3 devices?
   - ✓ A. ERSPAN
   - B. RSPAN

2. What is a common best practice when using RSPAN?
   - A. Tag mirrored traffic with a VLAN used for production traffic
   - ✓ B. Tag mirrored traffic with a dedicated VLAN used only for RSPAN

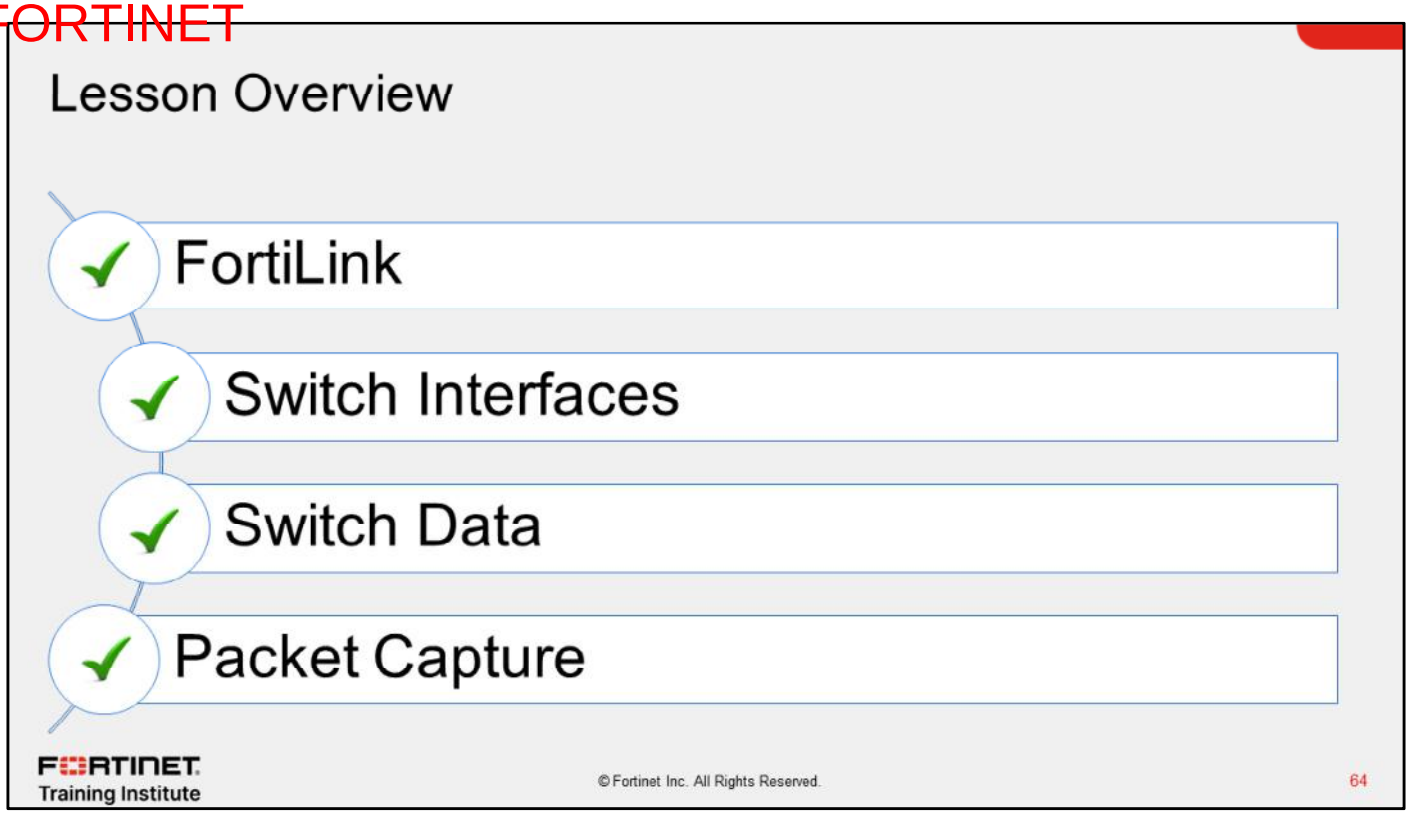
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

63

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

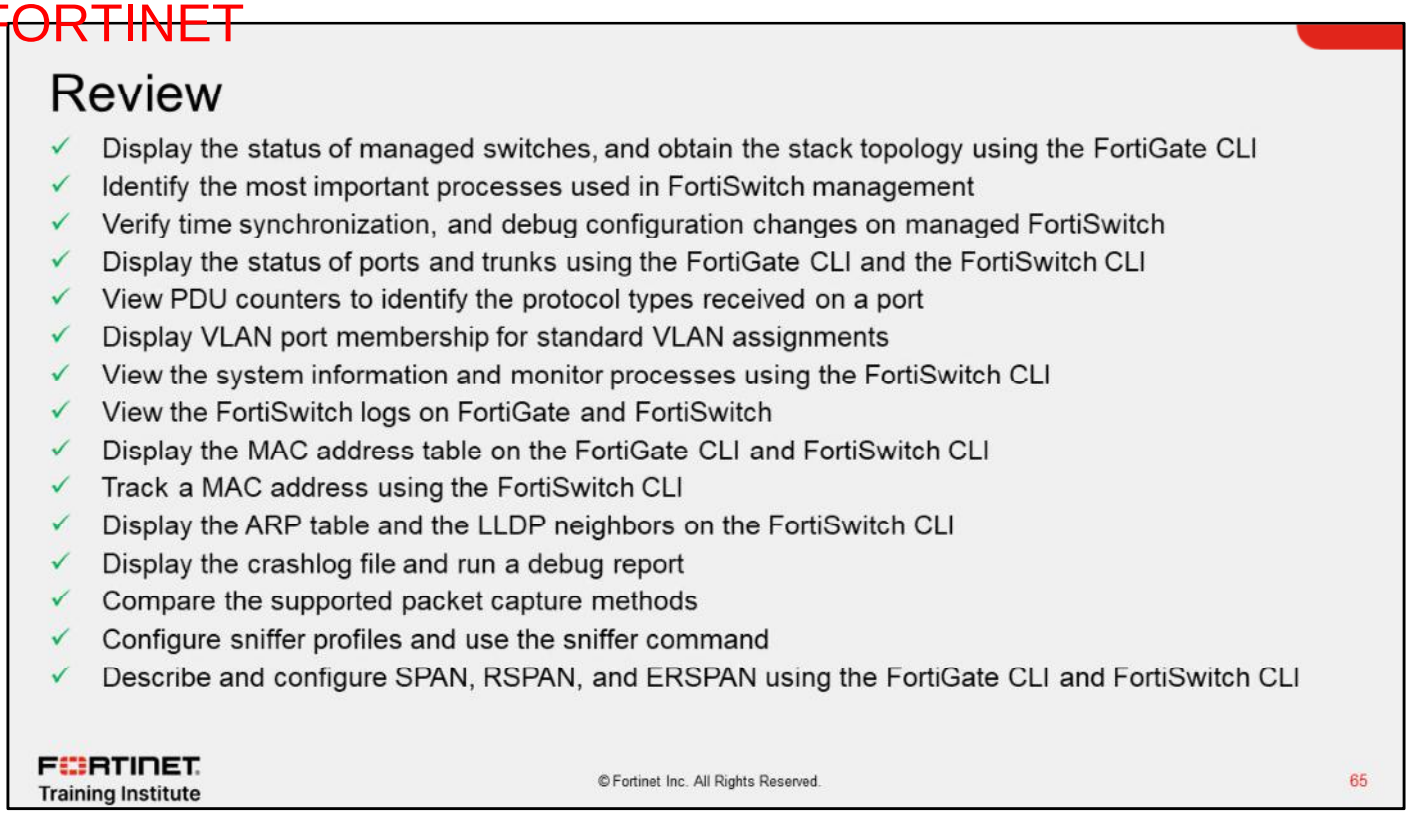


Good job! You now understand packet capture.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the most useful tools available to troubleshoot FortiSwitch issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923