Virtual Networks and VLANs

Amanda Bebin - ISDS
Colin Rhode - ISDS
Amy Blacketter - Graphic Design
Amanda Alfaro - CS

Objectives

- Define Virtual Network and VLAN
- Describe how they are used
- Break down their setup
- Discuss their advantages and disadvantages

Virtual Network (VNet)

- Network that consists of virtual network links
- Does not have physical connections/cables between devices
- Examples:
  - Amazon Virtual Private Cloud (VPC)
  - Microsoft Azure VNet

Virtual Local Area Network (VLAN)

- OSI Model: Layer 2 - Data Link
- Logical segmentation of a physical LAN into different broadcast domains
  - *Example: VoIP, Network Mgmt, SAN, Guest, DMZ, Datacenter, etc.*

Physical LAN

- Requires all users of the same requirements and same IP subnet (broadcast domain) be connected to the same equipment

VLAN

- Users can be spread out over various geographical locations and still remain in their same IP subnet (broadcast domain)

How to setup a Virtual Network

1. Pick your protocol

a. Point-to-Point Tunneling Protocol (PPTP)
- Pro – supported by all operating systems
- Con – least secure

b. Layer 2 Tunneling Protocol (L2TP)
- Pro – more secure then PPTP
- Con – more complicated to setup & has many of the same connection issues as the PPTP

c. Secure Sockets Layer (SSL)
- Very secure (banks & other secure domains use)
- Web browser-based

d. OpenVPN
- Pro - free & just as secure as SSL
- Con - requires a client to be installed & does not work on mobile

Examples for usage

Group all voice traffic on separate VLAN to prevent from adversely affecting routine client-server tasks

Allow visitors access to minimal network functions

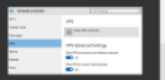
Reasons for usage

- Separating groups of users who need special security or network functions
- Isolating connections with heavy or unpredictable traffic patterns
- Identifying groups of devices whose data should be given priority handling
- Containing groups of devices that rely on legacy protocols incompatible with the majority of the network's traffic
- Separating a very large network into smaller, more manageable subnets

How to setup a Virtual Network

2. Setting up a simple VPN with Windows

a. Windows comes with a built-in client to connect securely to other Windows computers, but it only supports PPTP & L2TP



b. Search for VPN in Windows Search & then launch the VPN wizard when prompted

How to setup a Virtual Network

c. To connect to a commercial VPN, you must know the IP address of the network you are trying to connect to

d. To run your own VPN, find your own IP address by running the "ipconfig" command in Command Prompt

How to setup a Virtual Network

3. Use a third-party software to create a VPN server

a. Best when wanting to create a VPN between multiple computers to share files and resources without having to dedicate a PC to act as the VPN server or configure a router

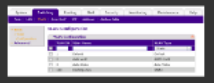
b. Examples of good third-party VPN software:
- Comodo Unite
- Gbridge
- TeamViewer

4. Purchase a VPN router

a. Zyxel
b. Cisco
c. Netgear

How to setup a VLAN

9. Select **Switching** > **VLAN** > **Basic** > **VLAN Configuration**



10. Create a static VLAN by specifying a **VLAN ID** & **name**
    - from the *VLAN Type* menu, select **Static**
11. Click the **Add** button
    - The new VLAN is added to the configuration

How to setup a VLAN

6. Select **Routing** > **IP** > **IP Configuration**
7. Next to *Routing Mode*, select the **Enable** radio button
8. Click the **Apply** button
    - Routing is now enabled

How to setup a VLAN

1. Determine the IP addresses that you want to assign to the VLAN interfaces on the switch
   - *For the switch to route between VLANs, the VLAN interfaces must have IP addresses. When the switch receives a packet that is destined for a VLAN or subnet, the switch forwards the packet to the destination VLAN interface based on the information in the routing table. The destination VLAN interface forwards the packet to the port to which the end device is attached.*
2. Open a web browser
3. In the browser *Address* field, type the IP address of the smart switch
   - Default IP address: 192.168.0.239
   - Default subnet mask: 255.255.255.0
4. Type the password in the *Password* field
   - Default password is ***password*** (case sensitive)
5. Click the **Login** button
   - After the system authenticates you, the *System Information* screen displays

How to setup a VLAN

12. Select **Routing** > **VLAN** > **VLAN Routing**

13. Enable routing on the VLAN that you just created & assign an IP address & subnet mask
    - From the *VLAN* menu, select the VLAN that you just created
    - In the *IP address* field, type the IP address that you want to assign to the VLAN routing interface
    - In the *Subnet Mask* field, type the subnet mask that you want to assign to the VLAN routing interface
    - In the *IP MTU* field, type **1500**
      - 1500 is the default MTU size
14. Click the **Add** button
    - The VLAN routing interface is added to the configuration & becomes active
15. Repeat Steps 9-14 for all VLANs that you want to designate as VLAN routing interfaces

Advantages of Virtual Networks

- Provides enhanced network security
- Easy to define
- Reduce the networking hardware investment (fewer cables, hubs) & eliminate dependencies on hardware
- Simplify management & access with centralized access control
- Consolidate hardware

Disadvantages of Virtual Networks

- Rely heavily on dedicated hardware
- Performance
- Data passed between virtual machines must be copied between their address spaces, adding further latency to the process

Advantages of VLANs

- Security
- Increased performance & bandwidth
- Improved manageability
- Reduced cost

Disadvantages of VLANs

- Management is complex
- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN but less efficient than a LAN

Virtual Networks and VLANs

Amanda Babin - ISDS
Colin Rhode - ISDS
Amy Blacketter - Graphic Design
Amanda Alfaro - CS

Objectives

- Define Virtual Network and VLAN
- Describe how they are used
- Break down their setup
- Discuss their advantages and disadvantages

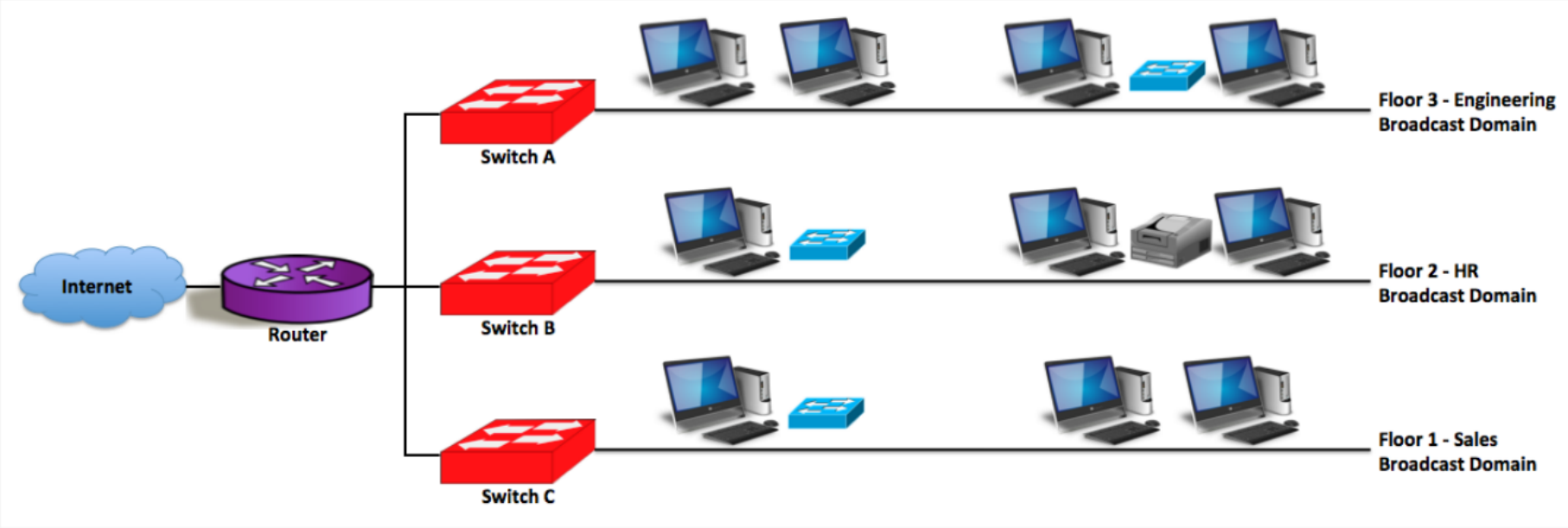
Virtual Network (VNet)

- Network that consists of virtual network links
- Does not have physical connections/cables between devices
- Examples:
  - Amazon Virtual Private Cloud (VPC)
  - Microsoft Azure VNet

Virtual Local Area Network (VLAN)

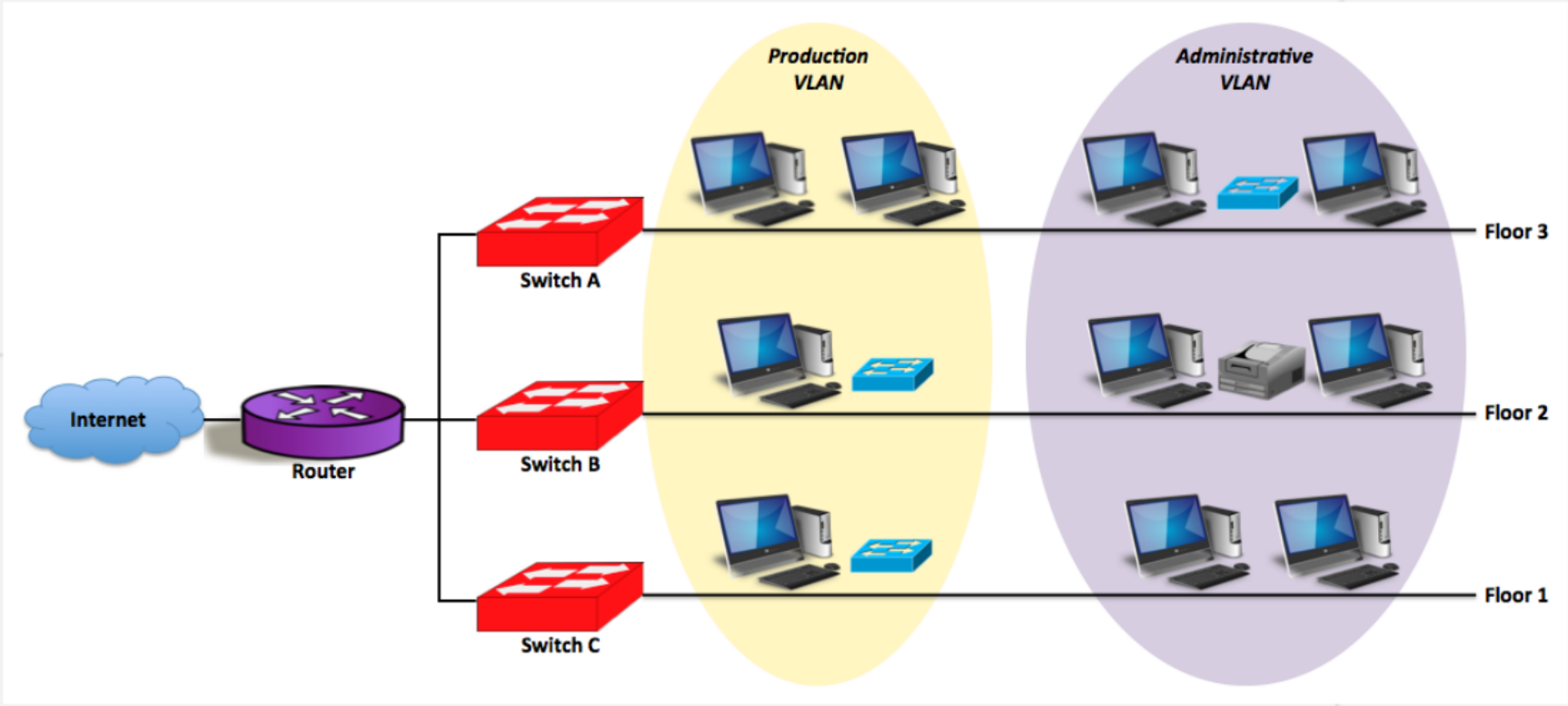
- OSI Model: Layer 2 - Data Link
- Logical segmentation of a physical LAN into different broadcast domains
  - *Example: VoIP, Network Mgmt, SAN, Guest, DMZ, Datacenter, etc.*

Physical LAN



- Requires all users of the same requirements and same IP subnet (broadcast domain) be connected to the same equipment

VLAN



- Users can be spread out over various geographical locations and still remain in their same IP subnet (broadcast domain)

Reasons for usage

- Separating groups of users who need special security or network functions
- Isolating connections with heavy or unpredictable traffic patterns
- Identifying groups of devices whose data should be given priority handling
- Containing groups of devices that rely on legacy protocols incompatible with the majority of the network's traffic
- Separating a very large network into smaller, more manageable subnets

Examples for usage

Group all voice traffic on separate VLAN to prevent from adversely affecting routine client-server tasks

Allow visitors access to minimal network functions

How to setup a Virtual Network

1. Pick your protocol

a. Point-to-Point Tunneling Protocol (PPTP)
- Pro – supported by all operating systems
- Con – least secure

b. Layer 2 Tunneling Protocol (L2TP)
- Pro – more secure then PPTP
- Con – more complicated to setup & has many of the same connection issues as the PPTP

c. Secure Sockets Layer (SSL)
- Very secure (banks & other secure domains use)
- Web browser-based

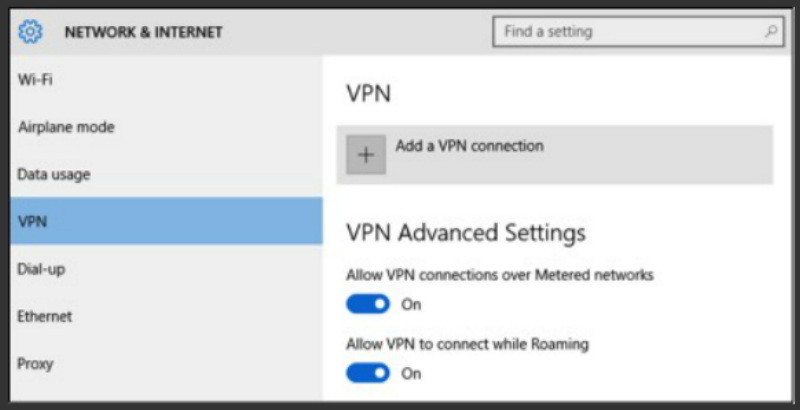
d. OpenVPN
- Pro - free & just as secure as SSL
- Con - requires a client to be installed & does not work on mobile

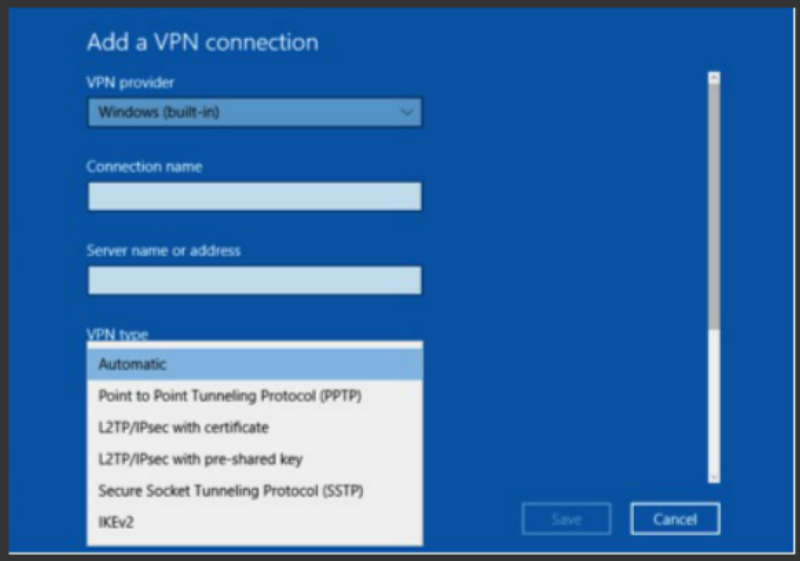
How to setup a Virtual Network

2. Setting up a simple VPN with Windows

a. Windows comes with a built-in client to connect securely to other Windows computers, but it only supports PPTP & L2TP

b. Search for VPN in Windows Search & then launch the VPN wizard when prompted

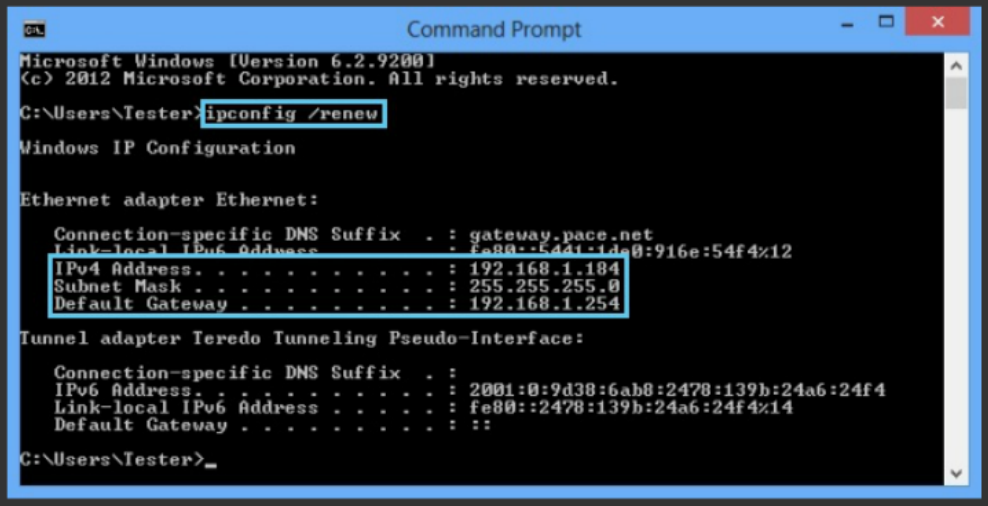




How to setup a Virtual Network

c. To connect to a commercial VPN, you must know the IP address of the network you are trying to connect to

d. To run your own VPN, find your own IP address by running the “ipconfig” command in Command Prompt



How to setup a Virtual Network

3. Use a third-party software to create a VPN server

a. Best when wanting to create a VPN between multiple computers to share files and resources without having to dedicate a PC to act as the VPN server or configure a router
b. Examples of good third-party VPN software:
- Comodo Unite
- Gbridge
- TeamViewer

4. Purchase a VPN router

a. Zyxel
b. Cisco
c. Netgear

How to setup a VLAN

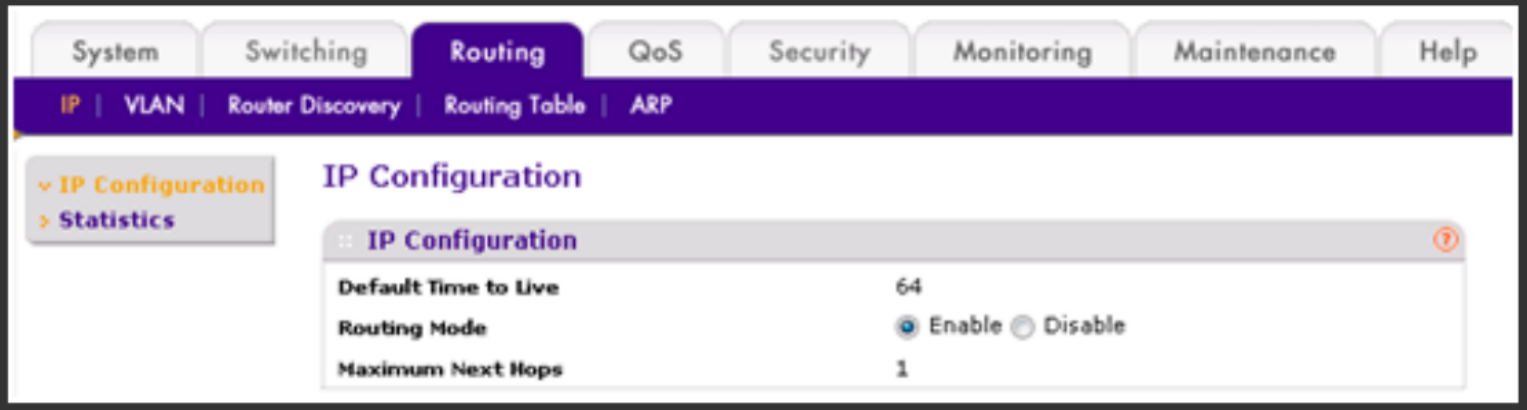
1. Determine the IP addresses that you want to assign to the VLAN interfaces on the switch
    - *For the switch to route between VLANs, the VLAN interfaces must have IP addresses. When the switch receives a packet that is destined for a VLAN or subnet, the switch forwards the packet to the destination VLAN interface based on the information in the routing table. The destination VLAN interface forwards the packet to the port to which the end device is attached.*
2. Open a web browser
3. In the browser *Address* field, type the IP address of the smart switch
    - Default IP address: 192.168.0.239
    - Default subnet mask: 255.255.255.0
4. Type the password in the *Password* field
    - Default password is ***password*** (case sensitive)
5. Click the **Login** button
    - After the system authenticates you, the *System Information* screen displays

How to setup a VLAN

6. Select **Routing** > **IP** > **IP Configuration**

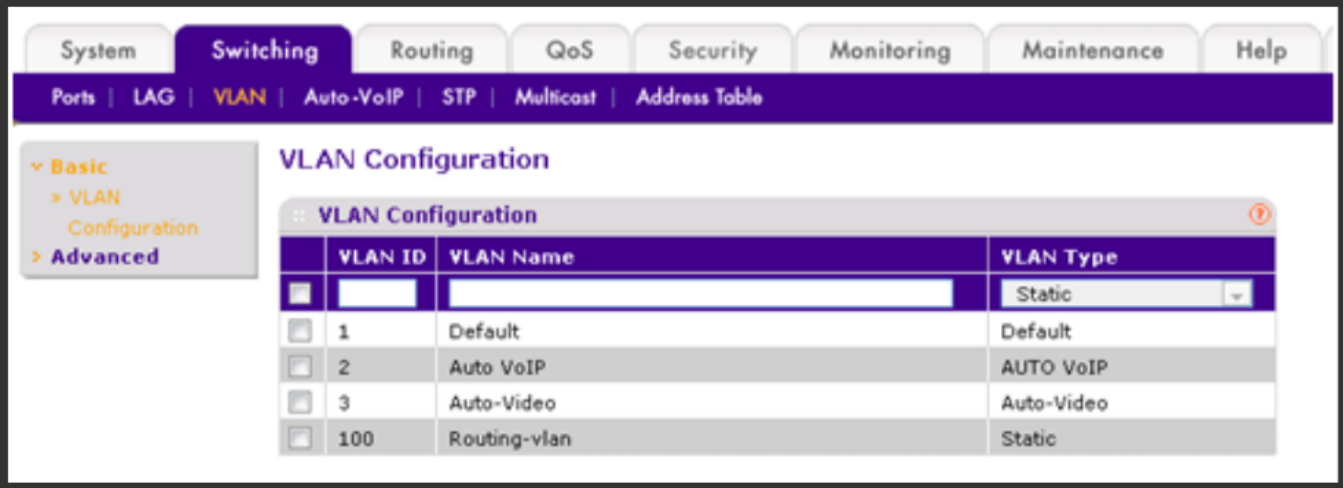
7. Next to *Routing Mode*, select the **Enable** radio button

8. Click the **Apply** button
    - Routing is now enabled



How to setup a VLAN

9. Select **Switching** > **VLAN** > **Basic** > **VLAN Configuration**

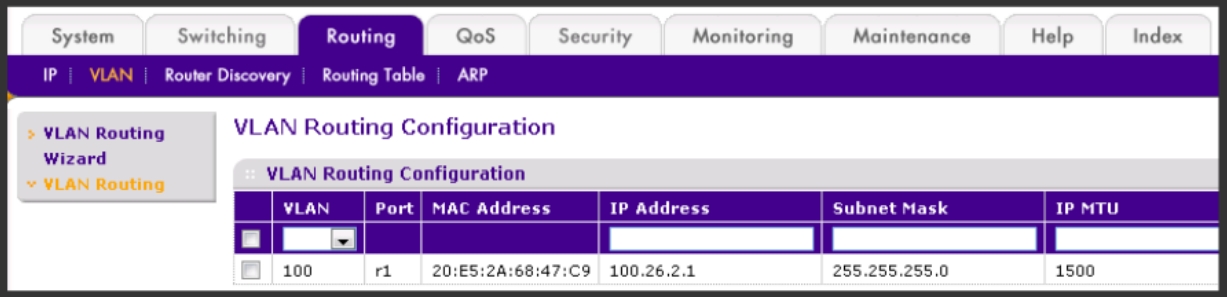


10. Create a static VLAN by specifying a **VLAN ID** & **name**
    - from the *VLAN Type* menu, select **Static**

11. Click the **Add** button
    - The new VLAN is added to the configuration

How to setup a VLAN

12. Select **Routing** > **VLAN** > **VLAN Routing**



13. Enable routing on the VLAN that you just created & assign an IP address & subnet mask
    - From the *VLAN* menu, select the VLAN that you just created
    - In the *IP address* field, type the IP address that you want to assign to the VLAN routing interface
    - In the *Subnet Mask* field, type the subnet mask that you want to assign to the VLAN routing interface
    - In the *IP MTU* field, type **1500**
        - 1500 is the default MTU size
14. Click the **Add** button
    - The VLAN routing interface is added to the configuration & becomes active
15. Repeat Steps 9-14 for all VLANs that you want to designate as VLAN routing interfaces

Advantages of Virtual Networks

- Provides enhanced network security
- Easy to define
- Reduce the networking hardware investment (fewer cables, hubs) & eliminate dependencies on hardware
- Simplify management & access with centralized access control
- Consolidate hardware

Disadvantages of Virtual Networks

- Rely heavily on dedicated hardware
- Performance
- Data passed between virtual machines must be copied between their address spaces, adding further latency to the process

Advantages of VLANs

- Security
- Increased performance & bandwidth
- Improved manageability
- Reduced cost

Disadvantages of VLANs

- Management is complex
- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN but less efficient than a LAN