WILEY

SYBEX
A Wiley Brand

CCNA Routing and Switching Study Guide

Chapters 2 &16: Network Device Management and Security

Instructor & Todd Lammle

Chapter 16 objectives

The ICND2 topics covered in this chapter include:

SYBEX
A Wiley Brand

The access layer

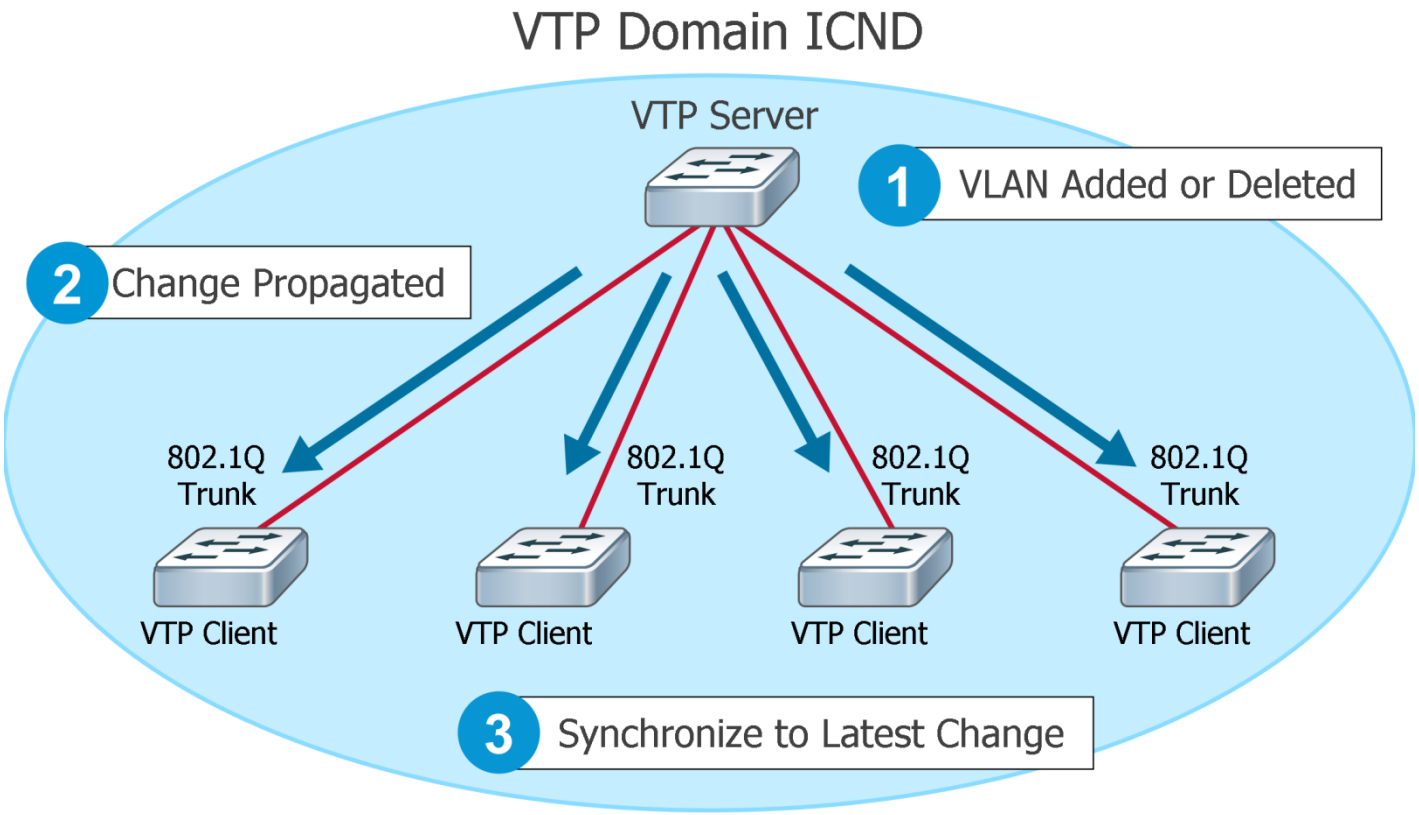
The following are some of the functions to be included at the access layer:

- Continued (from the distribution layer) use of access control and policies
- Creation of separate collision domains (microsegmentation/switches)
- Workgroup connectivity into the distribution layer
- Device connectivity
- Resiliency and security services
- Advanced technology capabilities (voice/video, PoE, port-security, etc.). Interfaces like Gigabit or FastEthernet switching frequently seen in the access layer

WILEY

SYBEX
A Wiley Brand

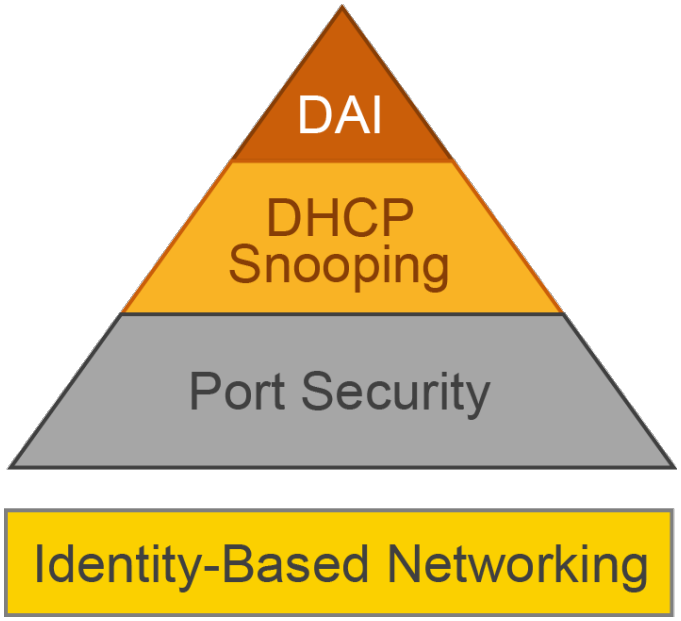
VTP



WILEY

SYBEX
A Wiley Brand

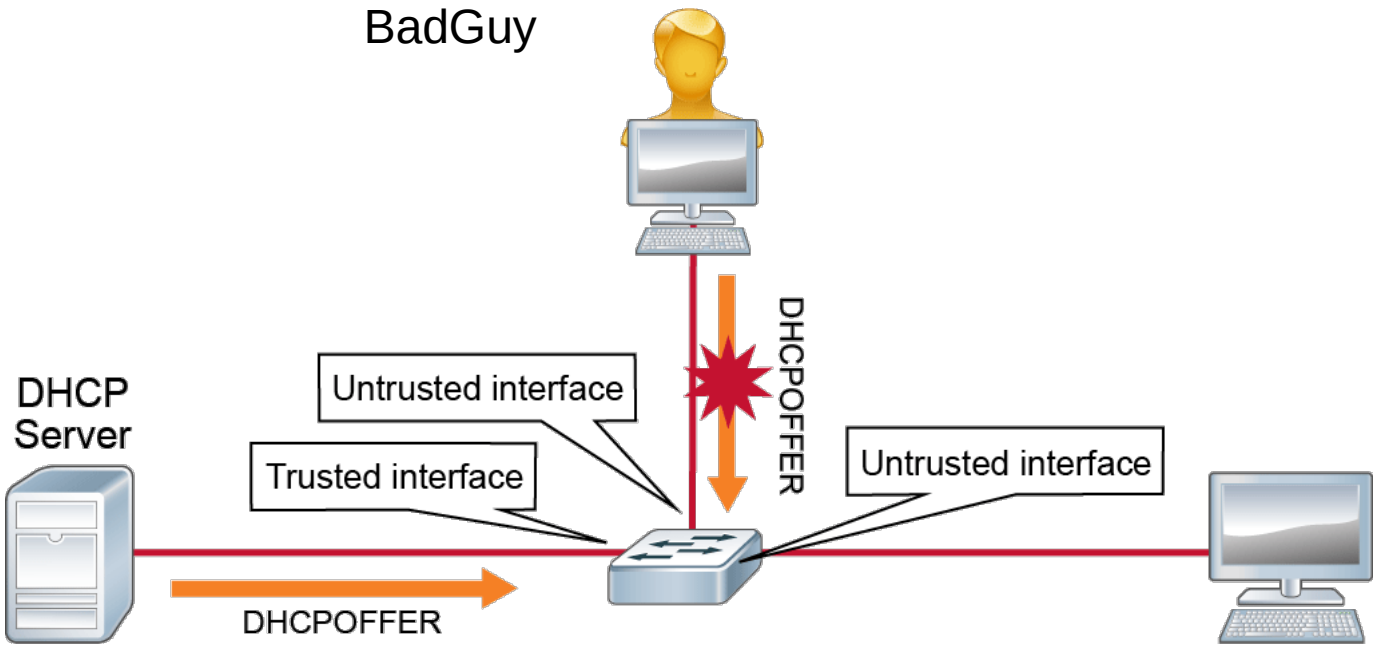
Mitigating threats at the access layer



WILEY

SYBEX
A Wiley Brand

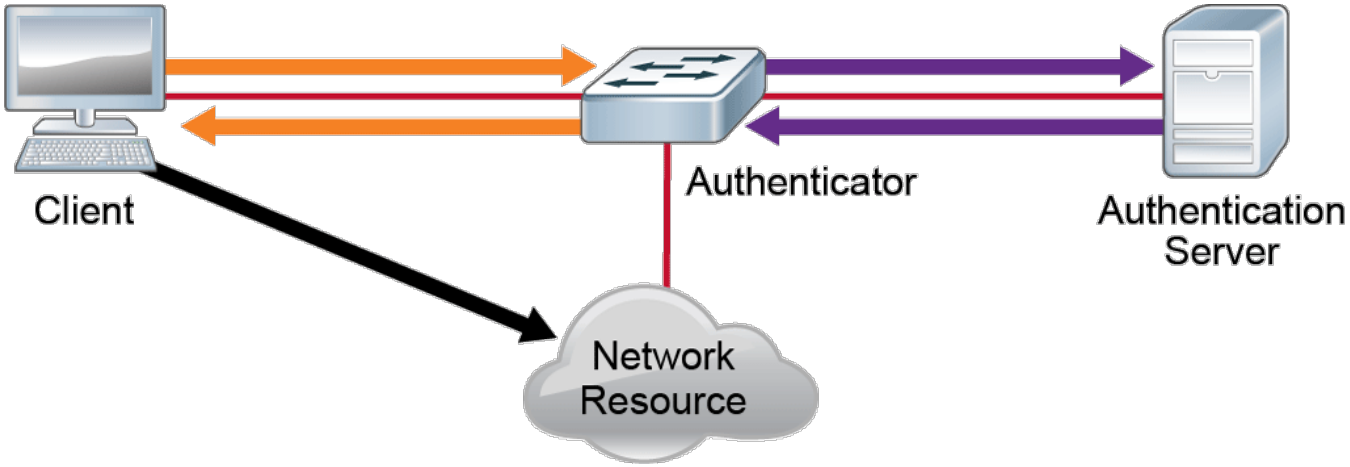
DHCP snooping and DAI



WILEY

SYBEX
A Wiley Brand

Identity-based networking



WILEY

SYBEX
A Wiley Brand

802.1x

The IEEE 802.1x standard allows you to implement identity-based networking on wired and wireless hosts by using client/server access control. There are three roles:

Client

Also referred to as a supplicant, this software runs on a client that is 802.1x compliant.

Authenticator

Typically a switch, this controls physical access to the network and is a proxy between the client and the authentication server.

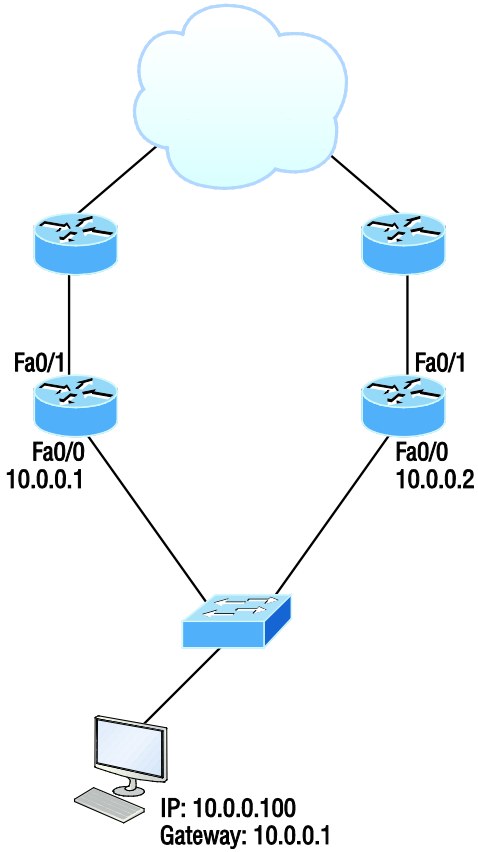
Authentication server (RADIUS)

This is a server that authenticates each client before making available any services.

WILEY

SYBEX
A Wiley Brand

Default gateway

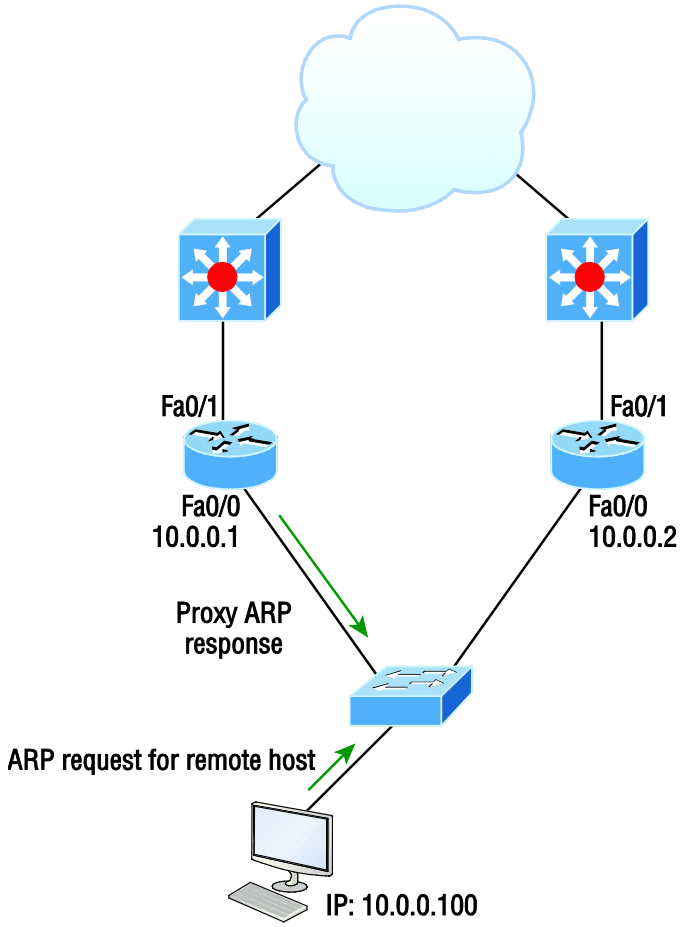


If you're wondering how you can possibly configure a client to send data off its local link when its default gateway router has gone down, you've targeted a key issue because the answer is that usually, you can't!

WILEY

SYBEX
A Wiley Brand

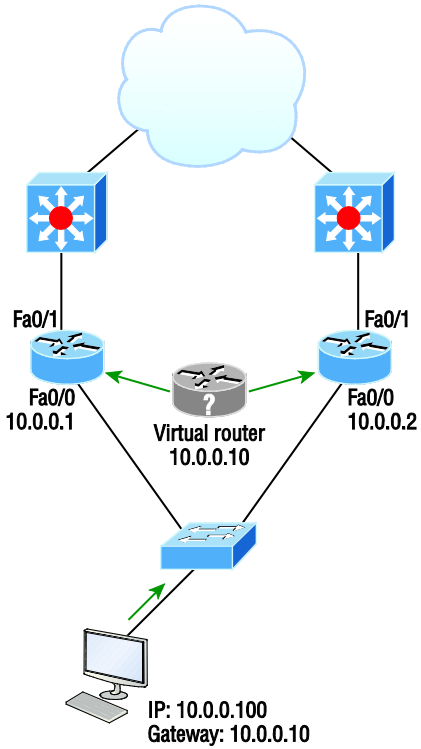
Proxy ARP



If a Proxy ARP–enabled router receives an ARP request for an IP address that it knows isn't on the same subnet as the requesting host, it will respond with an ARP reply packet to the host.

WILEY

FHRPs use a virtual router with a virtual IP address and virtual MAC address.

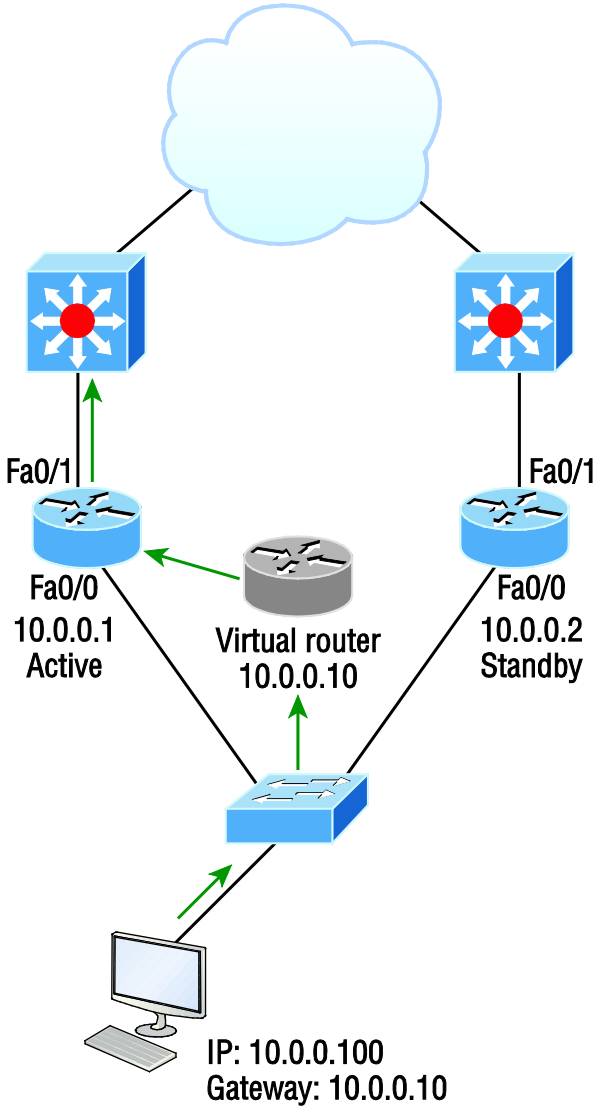


First hop redundancy protocols (FHRPs) work by giving you a way to configure more than one physical router to appear as if they were only a single logical one.

HSRP

HSRP is a Cisco proprietary protocol that can be run on most, but not all, of Cisco's router and multilayer switch models. It defines a standby group, and each standby group that you define includes the following routers:

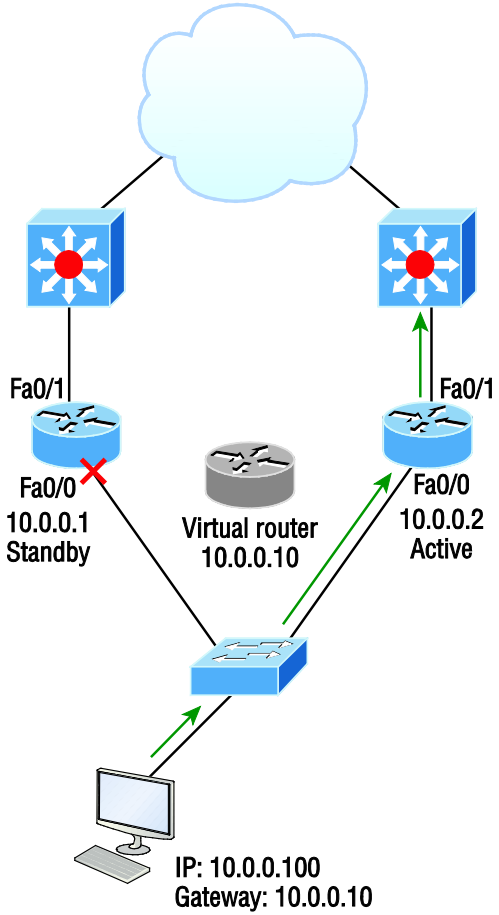
- Active router
- Standby router
- Virtual router
- Any other routers that maybe attached to the subnet



HSRP active and standby routers

The problem with HSRP is that with it, only one router is active and two or more routers just sit there in standby mode and won't be used unless a failure occurs—not very cost effective or efficient!

The standby group will always have at least two routers participating in it. The primary players in the group are the one active router and one standby router that communicate to each other using multicast Hello messages.



HSRP virtual MAC

The HSRP MAC address has only one variable piece in it. The first 24 bits still identify the vendor who manufactured the device (the organizationally unique identifier, or OUI).

The next 16 bits in the address tells us that the MAC address is a well-known HSRP MAC.

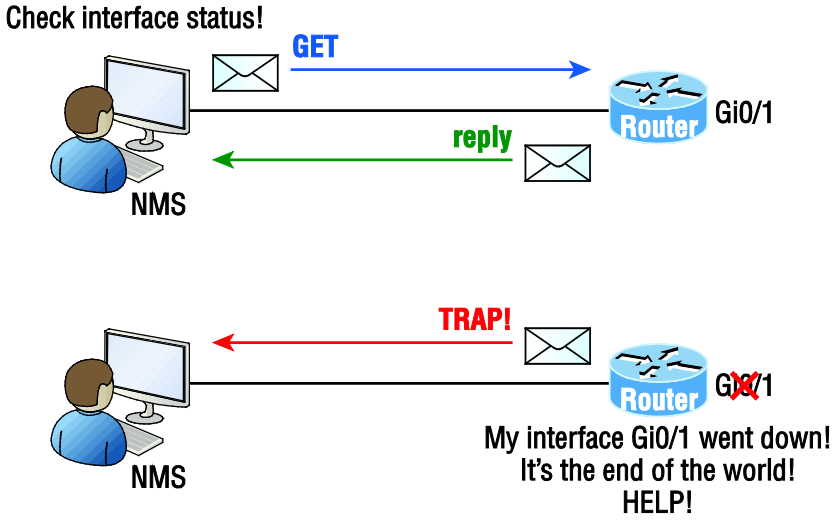
Here is an example of what an HSRP MAC address would look like:

```
0000.0c07.ac0a
```

- The first 24 bits (0000.0c) are the vendor ID of the address; in the case of HSRP being a Cisco protocol, the ID is assigned to Cisco.
- The next 16 bits (07.ac) are the well-known HSRP ID. This part of the address was assigned by Cisco in the protocol, so it's always easy to recognize that this address is for use with HSRP.
- The last 8 bits (0a) are the only variable bits and represent the HSRP group number that you assign. In this case, the group number is 10 and converted to hexadecimal when placed in the MAC address, where it becomes the 0a that you see.

SNMP

SNMP is an application layer protocol that provides a message format for agents on a variety of devices to communicate with network management stations (NMSs)



The NMS periodically queries or polls the SNMP agent on a device to gather and analyze statistics via GET messages. End devices running SNMP agents would send an SNMP trap to the NMS if a problem occurs.

SYBEX
A Wiley Brand

SNMP versions

SNMP has three versions, with version 1 being rarely, if ever implemented today. Here's a summary of these three versions:

SNMPv1
Supports plaintext authentication with community strings and uses only by UDP.

SNMPv2c
Supports plaintext authentication (using community strings) with MD5 or SHA with no encryption but provides GET BULK, which is a way to gather many types of information at once and minimize the number of GET requests. It offers a more detailed error message reporting method, but it's not more secure than v1. It uses UDP even though it can be configured to use TCP.

SNMPv3
Supports strong authentication with MD5 or SHA, providing confidentiality (encryption) and data integrity of messages via DES or DES-256 encryption between agents and managers. GET BULK is a supported feature of SNMPv3, and this version also uses TCP.

WILEY

Written labs and review questions

- Read through the Exam Essentials section together in class.
- Open your books and go through all the written labs and the review questions.
- Review the answers in class.