# F5 101 - Application Delivery Fundamentals Exam Overview

F5 101 - Application Delivery Fundamentals Exam

Based on Blueprint published 2019 reviewed 2024

Brandon Morgan – br.morgan@f5.com

Wi-Fi: **Ritz-Carlton_CONFERENCE**

Access Code: **f5wired**

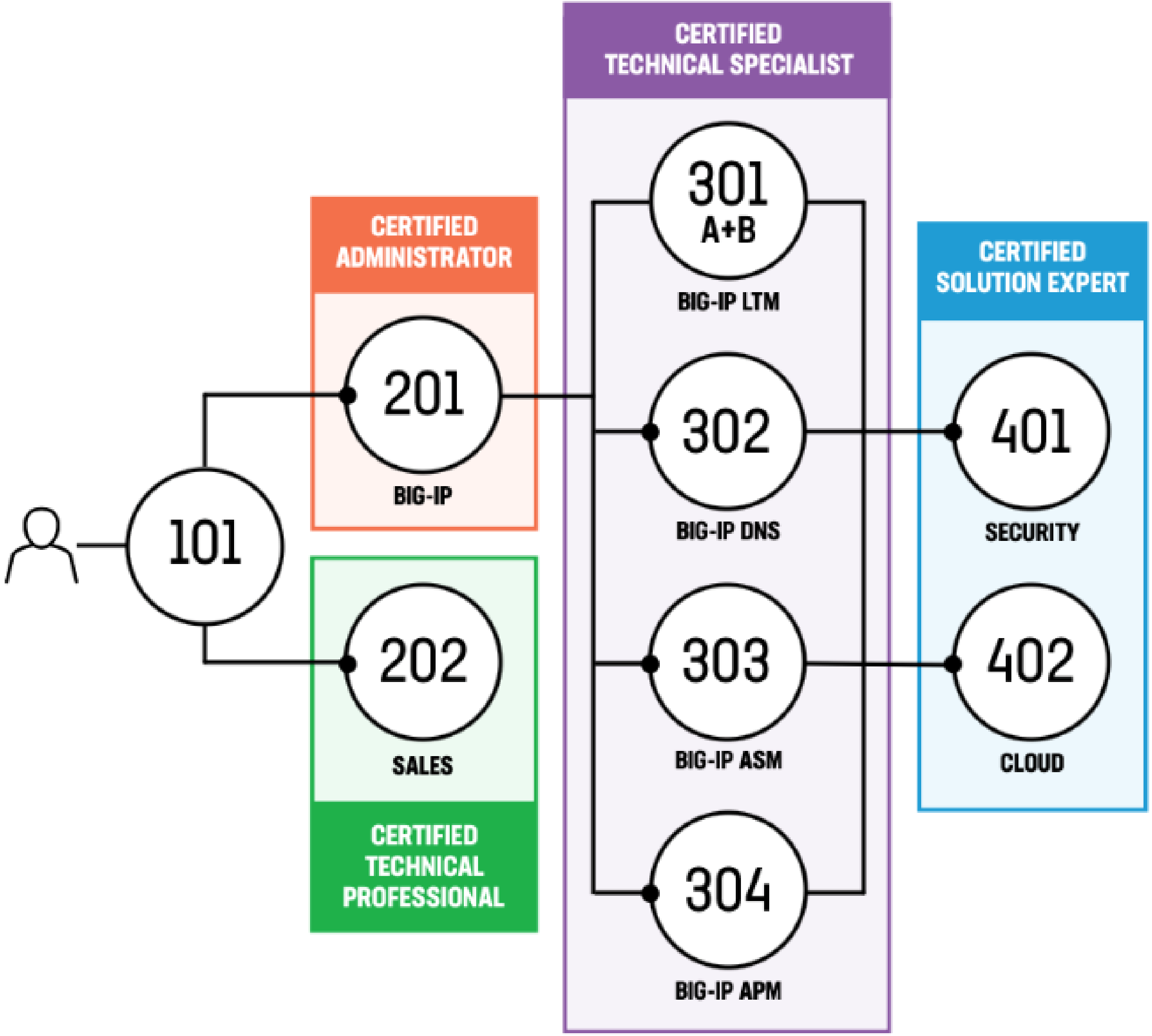
**Exam Issue:**

**support@mail.education.f5.com**

**Requesting Practice Exams:**

**s.Lopatin@f5.com**

# F5 Certifications & Exams



CERTIFIED ADMINISTRATOR

201 BIG-IP

101

202 SALES

CERTIFIED TECHNICAL PROFESSIONAL

CERTIFIED TECHNICAL SPECIALIST

301 A+B BIG-IP LTM

302 BIG-IP DNS

303 BIG-IP ASM

304 BIG-IP APM

CERTIFIED SOLUTION EXPERT

401 SECURITY

402 CLOUD

**F5 offers four certification tracks covering different job roles—Administration, Sales, Product Specialization, and Solutions Engineering. Choose the path that suits your needs and the depth of expertise required for your career or industry.**

### Administrator Track

Completion of an Administrator track validates that you have the fundamental knowledge necessary to manage, maintain, and do basic fault isolation of previously installed and configured F5 products or solutions.

### Technical Professional Track

Completion of a Technical Professional track validates that you have the skills, understanding, and specialized knowledge of F5 solutions, allowing you to more effectively contribute to the F5 ecosystem.

### Technical Specialist Track

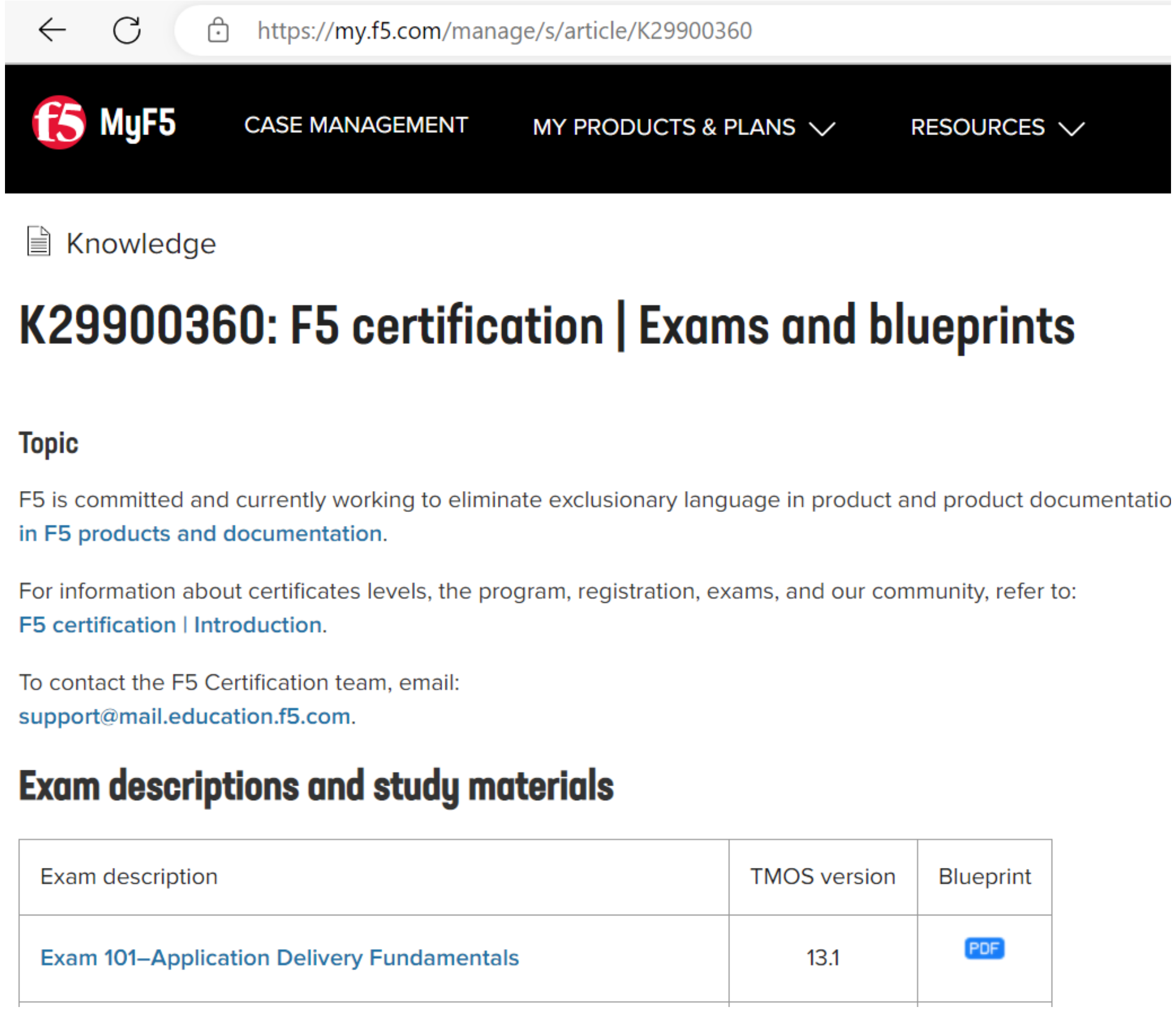
Completion of a Technical Specialist track validates that you have the expert-level knowledge needed to design, implement, and troubleshoot a specific F5 product as part of an overall solution.

### Solution Expert Track

Completion of a Solution Expert track validates that you have the expert-level knowledge needed to architect and design complex, integrated solutions with multiple F5 products and industry standards aligned with business and technical requirements.

# F5 101 Application Delivery Fundamentals

All Blueprints - https://my.f5.com/manage/s/article/K29900360



Knowledge

## K29900360: F5 certification | Exams and blueprints

### Topic

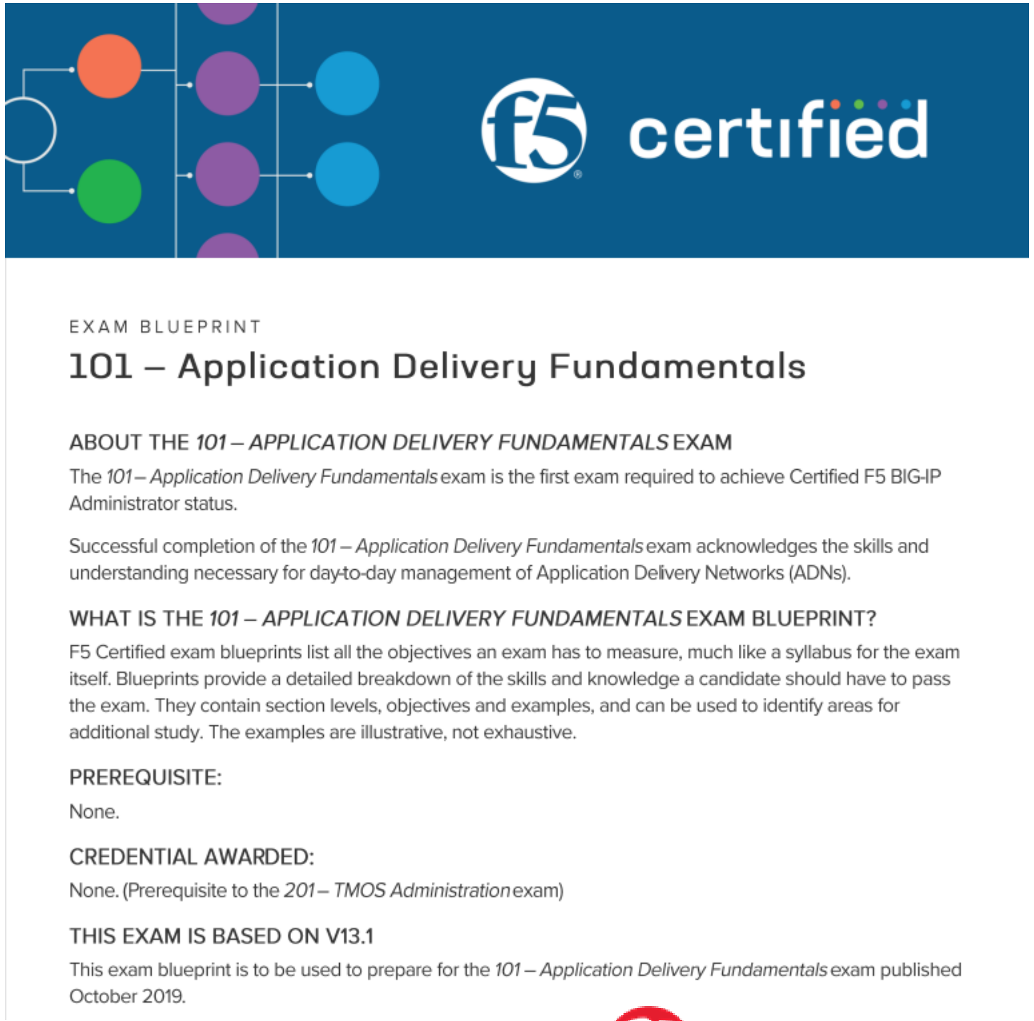
F5 is committed and currently working to eliminate exclusionary language in product and product documentatio in F5 products and documentation.

For information about certificates levels, the program, registration, exams, and our community, refer to: F5 certification | Introduction.

To contact the F5 Certification team, email: support@mail.education.f5.com.

### Exam descriptions and study materials

| Exam description | TMOS version | Blueprint |
|---|---|---|
| Exam 101–Application Delivery Fundamentals | 13.1 | PDF |



EXAM BLUEPRINT

## 101 – Application Delivery Fundamentals

ABOUT THE *101 – APPLICATION DELIVERY FUNDAMENTALS* EXAM

The *101 – Application Delivery Fundamentals* exam is the first exam required to achieve Certified F5 BIG-IP Administrator status.

Successful completion of the *101 – Application Delivery Fundamentals* exam acknowledges the skills and understanding necessary for day-to-day management of Application Delivery Networks (ADNs).

WHAT IS THE *101 – APPLICATION DELIVERY FUNDAMENTALS* EXAM BLUEPRINT?

F5 Certified exam blueprints list all the objectives an exam has to measure, much like a syllabus for the exam itself. Blueprints provide a detailed breakdown of the skills and knowledge a candidate should have to pass the exam. They contain section levels, objectives and examples, and can be used to identify areas for additional study. The examples are illustrative, not exhaustive.

PREREQUISITE:

None.

CREDENTIAL AWARDED:

None. (Prerequisite to the *201 – TMOS Administration* exam)

THIS EXAM IS BASED ON V13.1

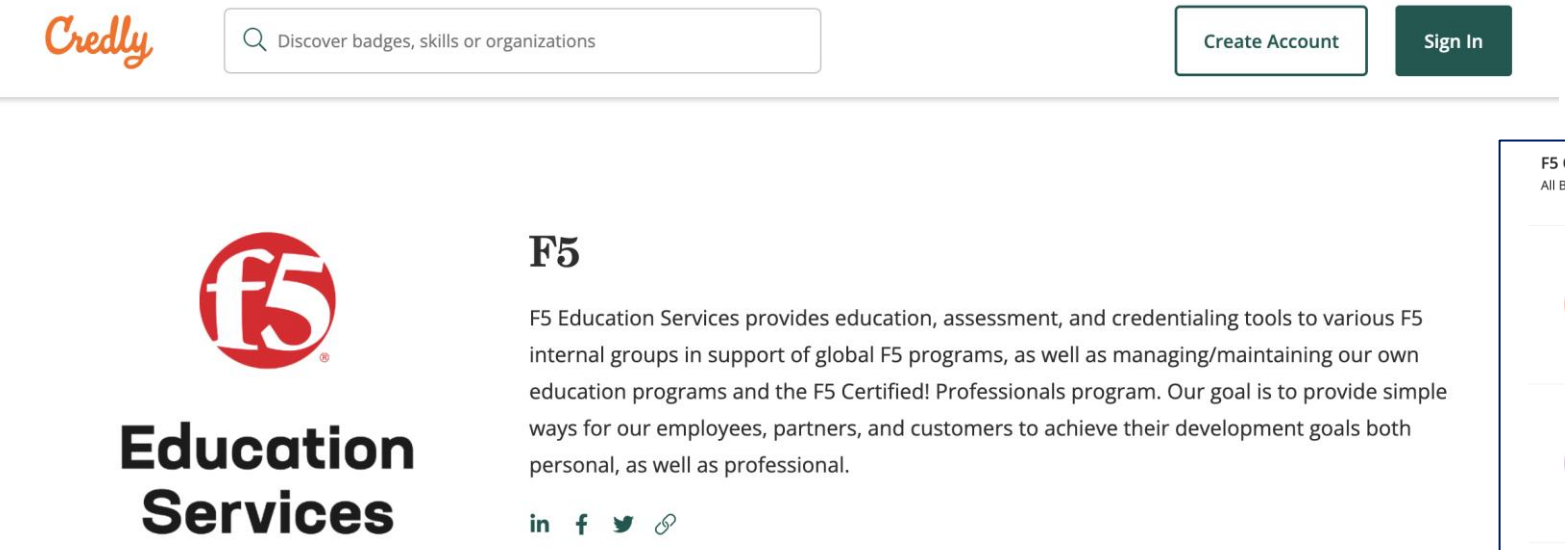
This exam blueprint is to be used to prepare for the *101 – Application Delivery Fundamentals* exam published October 2019.

# F5 Certification Exam Structure and Delivery

F5 101 exam - Application Delivery Fundamentals

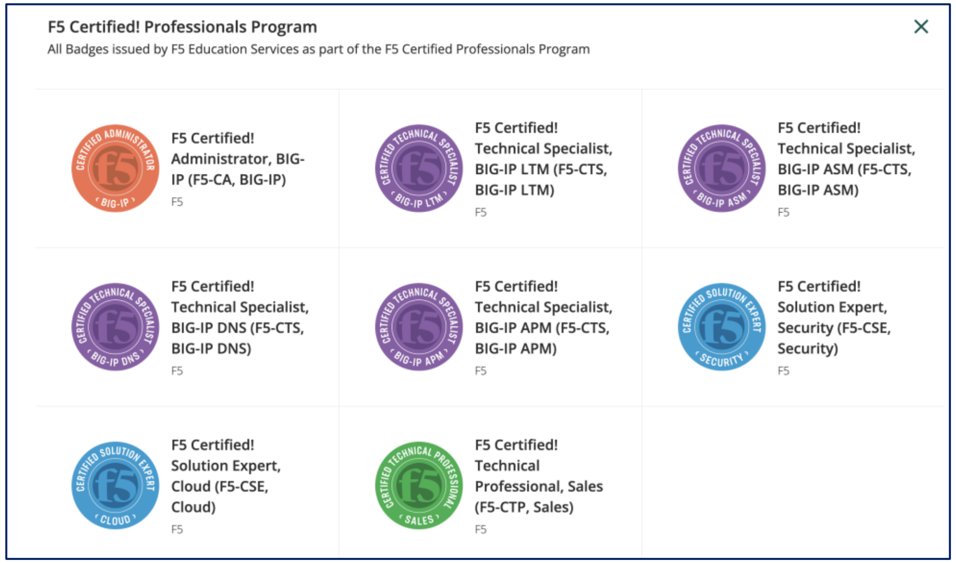
- The 101 and 201 exams are 90 minutes in duration.
- The 101 and 201 exams each have 80 questions.
- The questions are all multiple choice.
  - There are no true/false questions.
  - There are no “all of the above/none of the above” questions.
- The questions are not adaptive.
- Some questions have exhibits. It is best to view the entire exhibit to answer the question.
- Questions can be flagged, reviewed and re-answered within the 90-minute exam time limit.
- Exams are delivered at Pearson VUE testing centers and events like the Public Sector Symposium.
  - Exams taken at the Public Sector Symposium will be delivered this Thursday.
  - Exams will be delivered on iPads in a quiet room at this venue.
- Government-issued IDs are required to take exams.

# F5 Certification Badges



F5

F5 Education Services provides education, assessment, and credentialing tools to various F5 internal groups in support of global F5 programs, as well as managing/maintaining our own education programs and the F5 Certified! Professionals program. Our goal is to provide simple ways for our employees, partners, and customers to achieve their development goals both personal, as well as professional.



F5 Certified! Professionals Program

All Badges issued by F5 Education Services as part of the F5 Certified Professionals Program

- F5 Certified! Administrator, BIG-IP (F5-CA, BIG-IP) F5
- F5 Certified! Technical Specialist, BIG-IP LTM (F5-CTS, BIG-IP LTM) F5
- F5 Certified! Technical Specialist, BIG-IP ASM (F5-CTS, BIG-IP ASM) F5
- F5 Certified! Technical Specialist, BIG-IP DNS (F5-CTS, BIG-IP DNS) F5
- F5 Certified! Technical Specialist, BIG-IP APM (F5-CTS, BIG-IP APM) F5
- F5 Certified! Solution Expert, Security (F5-CSE, Security) F5
- F5 Certified! Solution Expert, Cloud (F5-CSE, Cloud) F5
- F5 Certified! Technical Professional, Sales (F5-CTP, Sales) F5

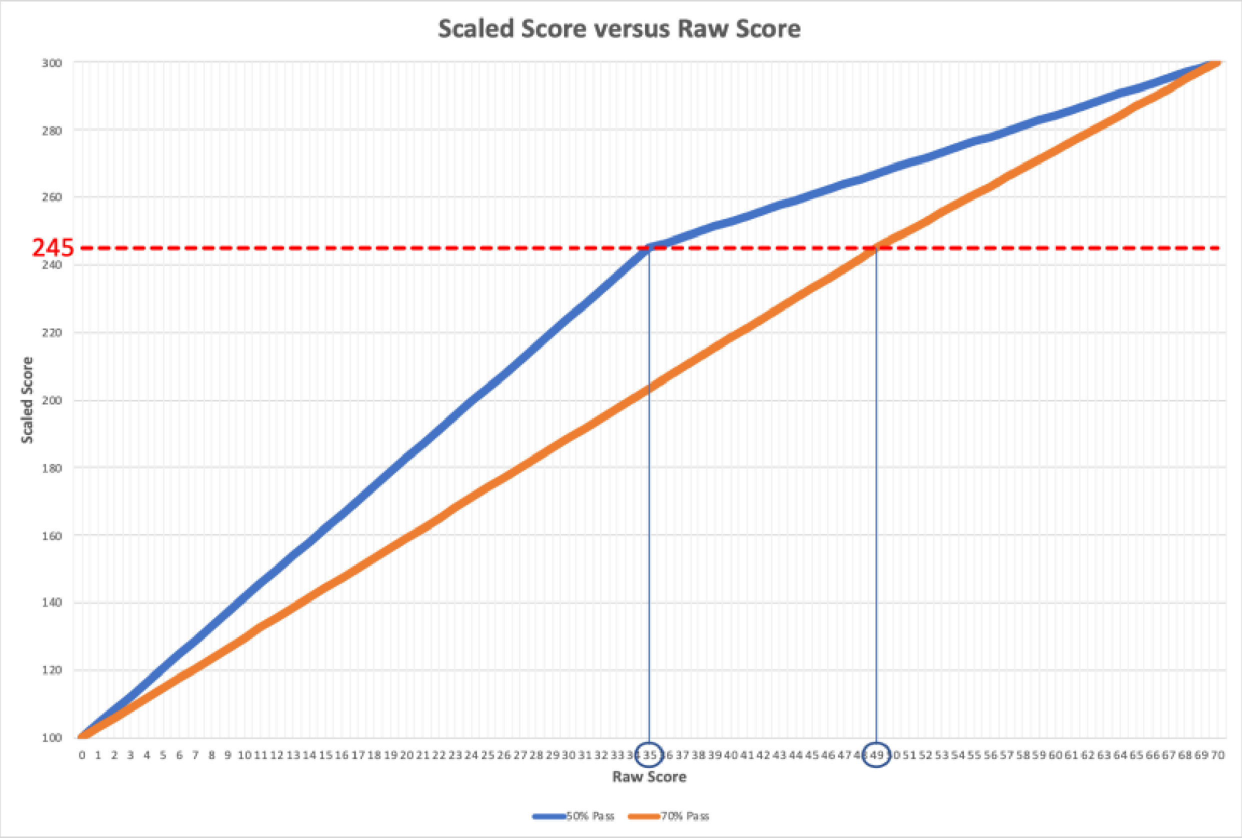
# F5 Certification Exams – Scaled Scoring

**PASS = 245**

How does scaled-scoring work?

Scaled-scoring is a method of score reporting that standardizes scores across exams, different exam forms, and exam versions.

Instead of reporting exam results as a percentage of total items answered correctly and having different required passing percentages for each exam, all F5 exams are scored on a scaled-score basis, where your score will range from a possible 100-350 points; all F5 exams are calibrated for a passing score of 245 on that scale.



https://education.f5.com/hc/en-us/articles/4403992805019-How-does-Scaled-Scoring-work-

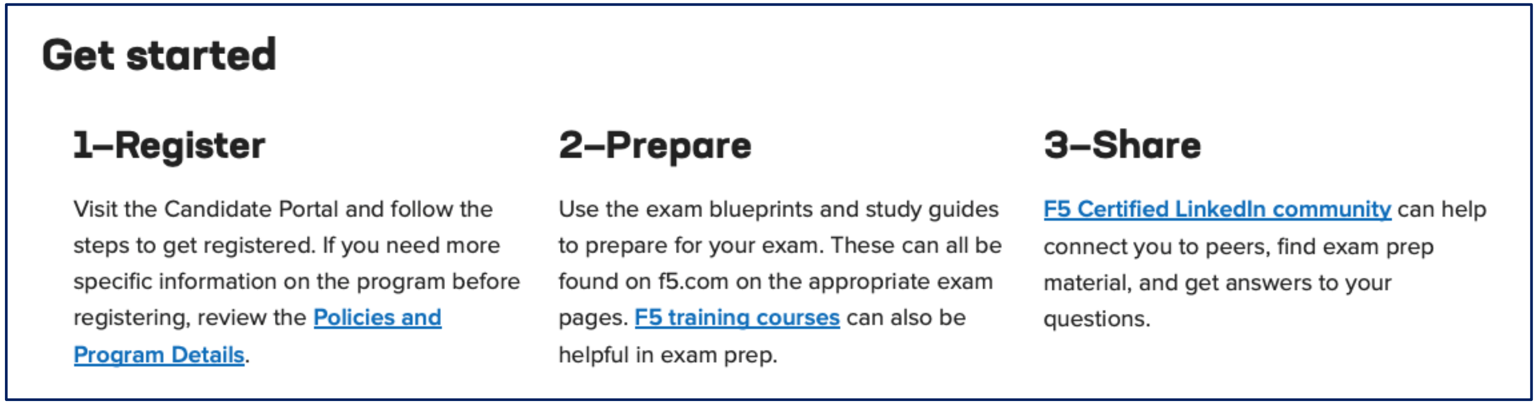
Questions? Email support@mail.education.f5.com

# F5 Certification Exam Retake Policy:

- After first failure, you must wait 15 days to re-test
- After second failure, you must wait 30 days to re-test
- After third failure, you must wait 45 days to re-test
- After fourth failure, you must wait 1 calendar year to re-test
- 5th and subsequent failed attempts, you must wait 90 days

# F5 Certification Candidate Registration (How do I get started?)

- https://www.f5.com/services/certification
- Scroll to the Candidate Portal link to register and create an account
- Fill out the form information
- Receive email with F5 Candidate ID
- Follow email instructions
- Register for exam today!



## Get started

### 1–Register

Visit the Candidate Portal and follow the steps to get registered. If you need more specific information on the program before registering, review the Policies and Program Details.

### 2–Prepare

Use the exam blueprints and study guides to prepare for your exam. These can all be found on f5.com on the appropriate exam pages. F5 training courses can also be helpful in exam prep.

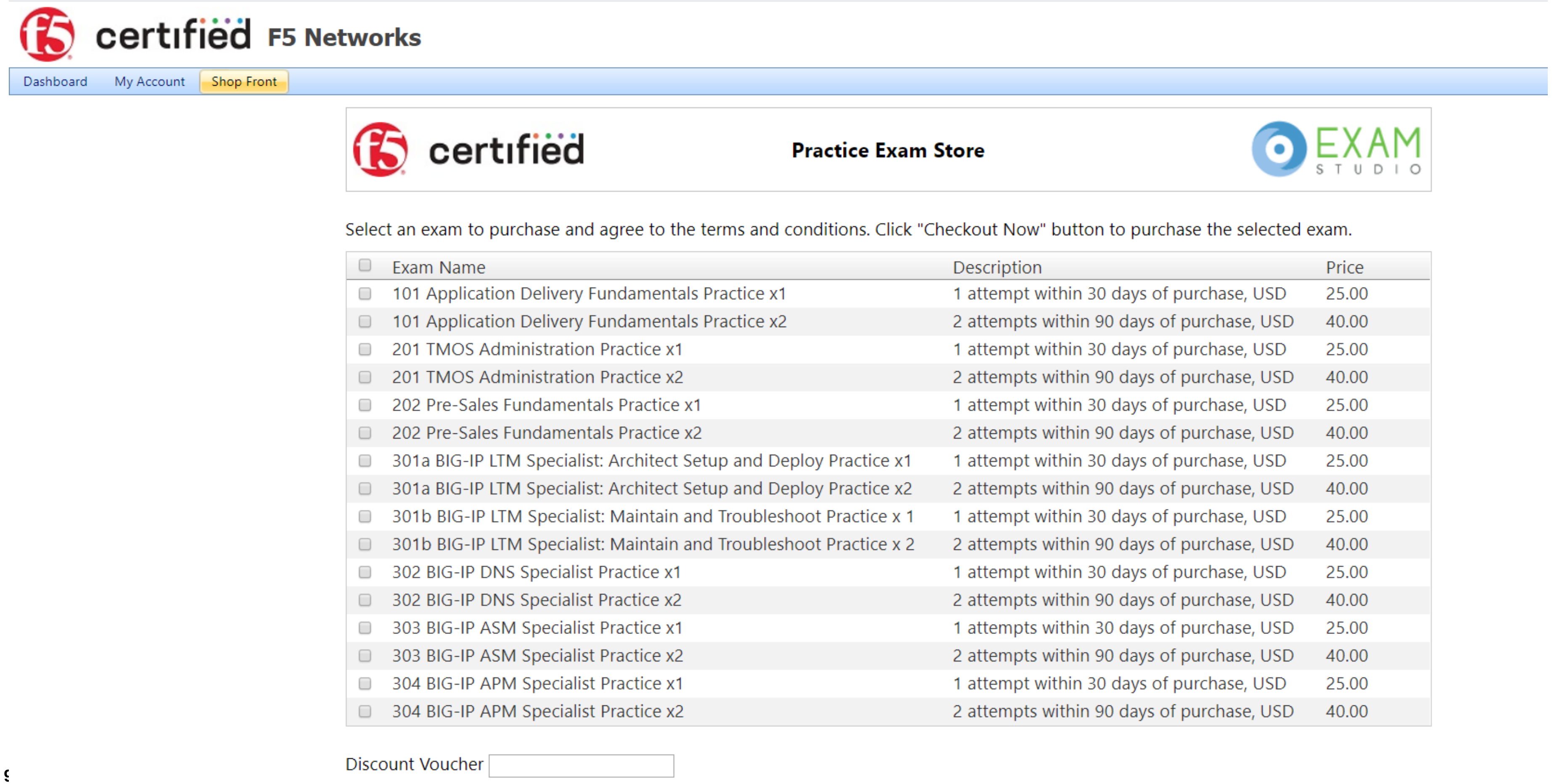
### 3–Share

F5 Certified LinkedIn community can help connect you to peers, find exam prep material, and get answers to your questions.

# Additional F5 Certification Resources

## Practice Exams through Zoomorphix at www.examstudio.com

You will be able to setup account through Cert Program Enrollment Process



Practice Exam Store

Select an exam to purchase and agree to the terms and conditions. Click "Checkout Now" button to purchase the selected exam.

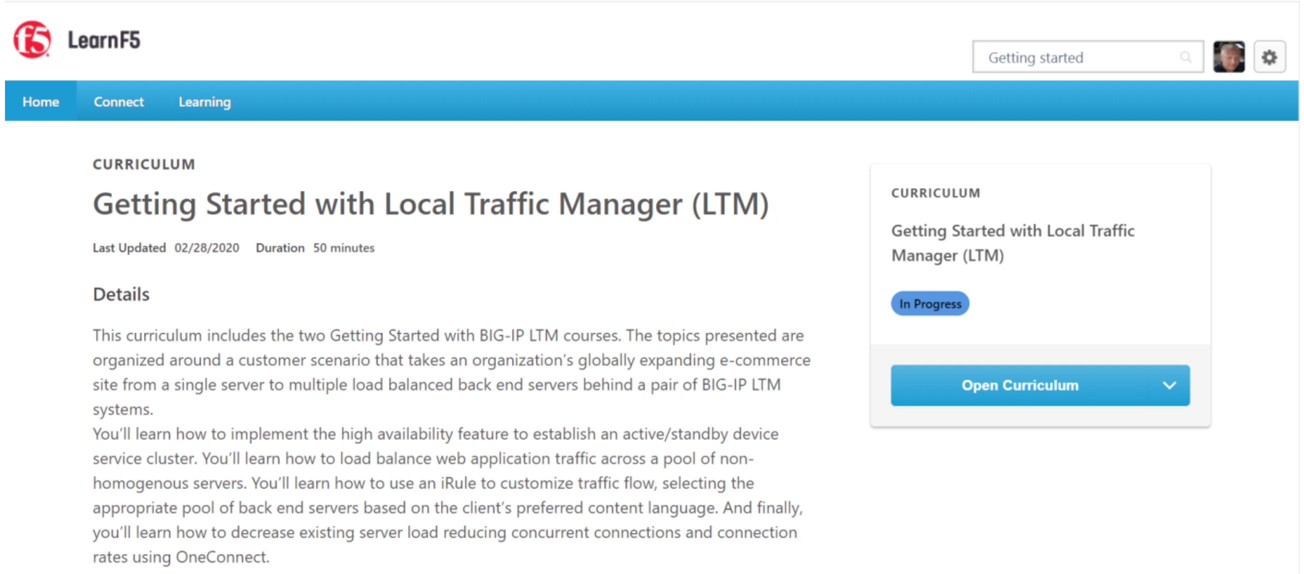
| □ | Exam Name | Description | Price |
|---|---|---|---|
| □ | 101 Application Delivery Fundamentals Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 101 Application Delivery Fundamentals Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 201 TMOS Administration Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 201 TMOS Administration Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 202 Pre-Sales Fundamentals Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 202 Pre-Sales Fundamentals Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 301a BIG-IP LTM Specialist: Architect Setup and Deploy Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 301a BIG-IP LTM Specialist: Architect Setup and Deploy Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 301b BIG-IP LTM Specialist: Maintain and Troubleshoot Practice x 1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 301b BIG-IP LTM Specialist: Maintain and Troubleshoot Practice x 2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 302 BIG-IP DNS Specialist Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 302 BIG-IP DNS Specialist Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 303 BIG-IP ASM Specialist Practice x1 | 1 attempts within 30 days of purchase, USD | 25.00 |
| □ | 303 BIG-IP ASM Specialist Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |
| □ | 304 BIG-IP APM Specialist Practice x1 | 1 attempt within 30 days of purchase, USD | 25.00 |
| □ | 304 BIG-IP APM Specialist Practice x2 | 2 attempts within 90 days of purchase, USD | 40.00 |

Discount Voucher

# Additional Resources

F5 Certified! Professionals

Listed group



CURRICULUM

Getting Started with Local Traffic Manager (LTM)

Last Updated 02/28/2020 Duration 50 minutes

Details

This curriculum includes the two Getting Started with BIG-IP LTM courses. The topics presented are organized around a customer scenario that takes an organization's globally expanding e-commerce site from a single server to multiple load balanced back end servers behind a pair of BIG-IP LTM systems.

You'll learn how to implement the high availability feature to establish an active/standby device service cluster. You'll learn how to load balance web application traffic across a pool of non-homogenous servers. You'll learn how to use an iRule to customize traffic flow, selecting the appropriate pool of back end servers based on the client's preferred content language. And finally, you'll learn how to decrease existing server load reducing concurrent connections and connection rates using OneConnect.

CURRICULUM

Getting Started with Local Traffic Manager (LTM)

In Progress

Open Curriculum

## Study groups on LinkedIn

| | |
|---|---|
| F5 Certified Professionals | https://www.linkedin.com/groups/85832 |
| LinkedIn – F5 Certified! – 101 | https://www.linkedin.com/groups/6711359/profile |
| LinkedIn – F5 Certified! – 201 | https://www.linkedin.com/groups/6709915/profile |

## Free online training courses

Getting Started with Local Traffic Manager

https://f5u.csod.com/ui/lms-learning-details/app/curriculum/b4332395-f110-48e1-9b86-5214e2e8165c

# Section 4: Knowledge

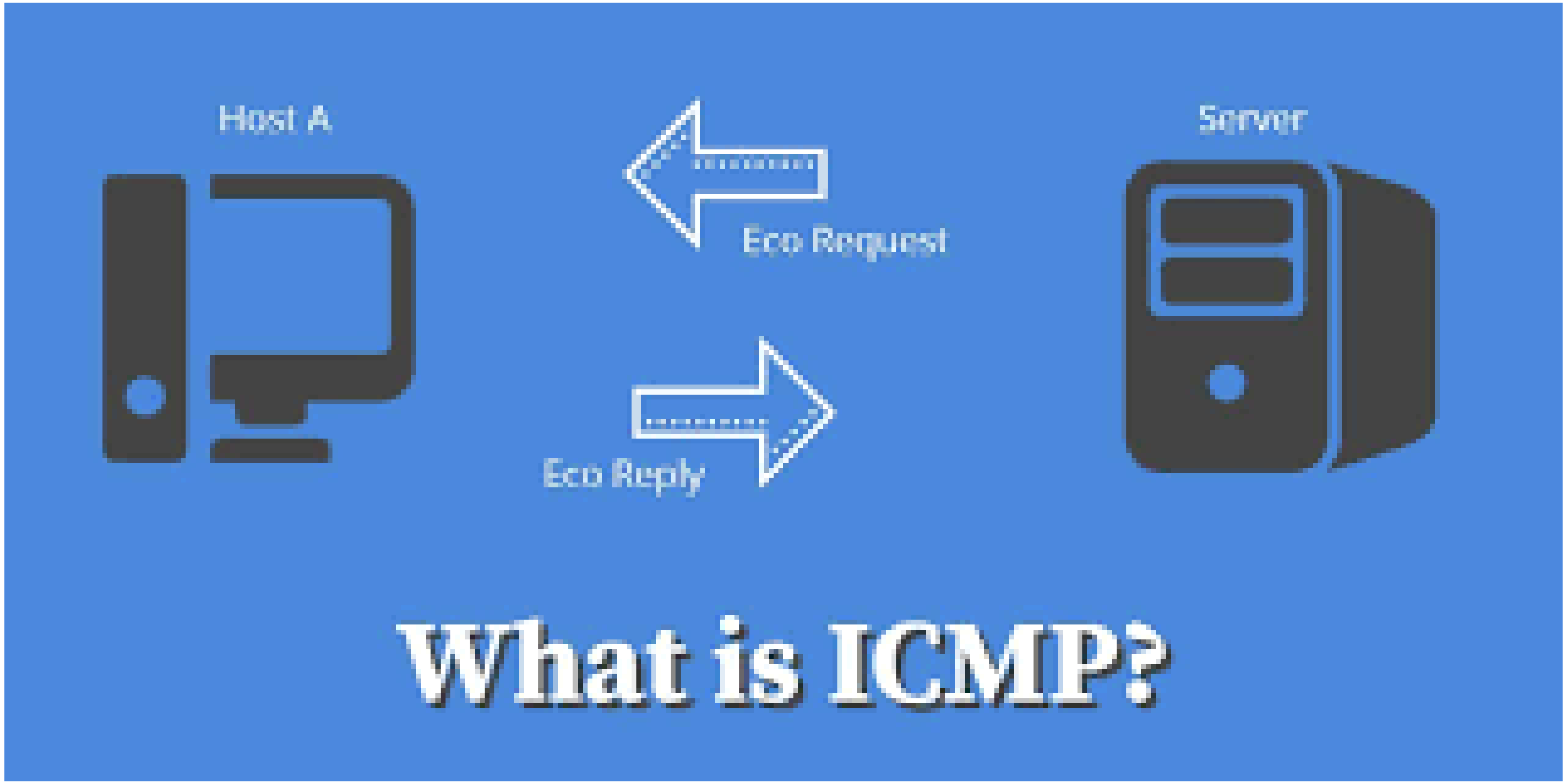
# Objective 4.01

## EXPLAIN COMMON USES FOR ICMP

- Explain the purpose of an IP TTL
- Explain the purpose of ICMP echo request/reply
- Explain reasons for ICMP unreachable

# Objective 4.01

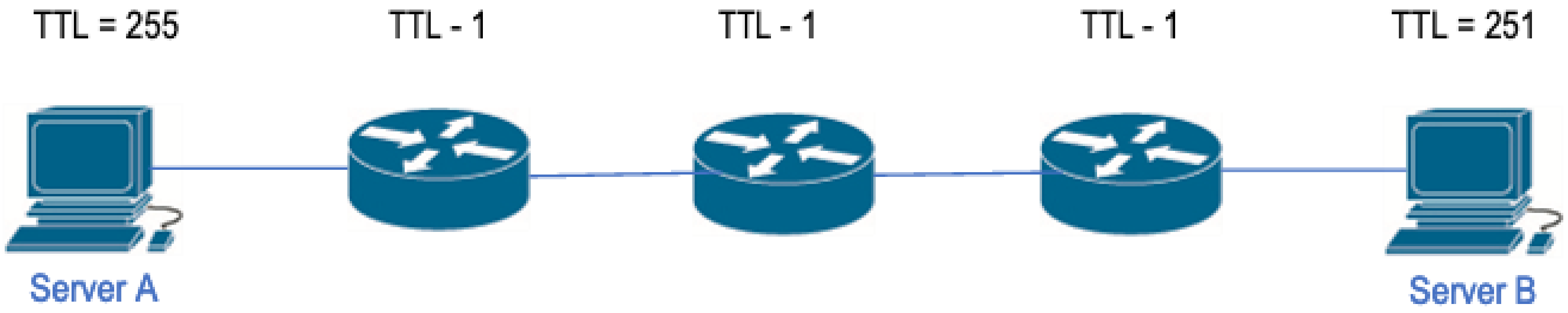
ICMP



# Objective 4.01

Explain common uses for ICMP

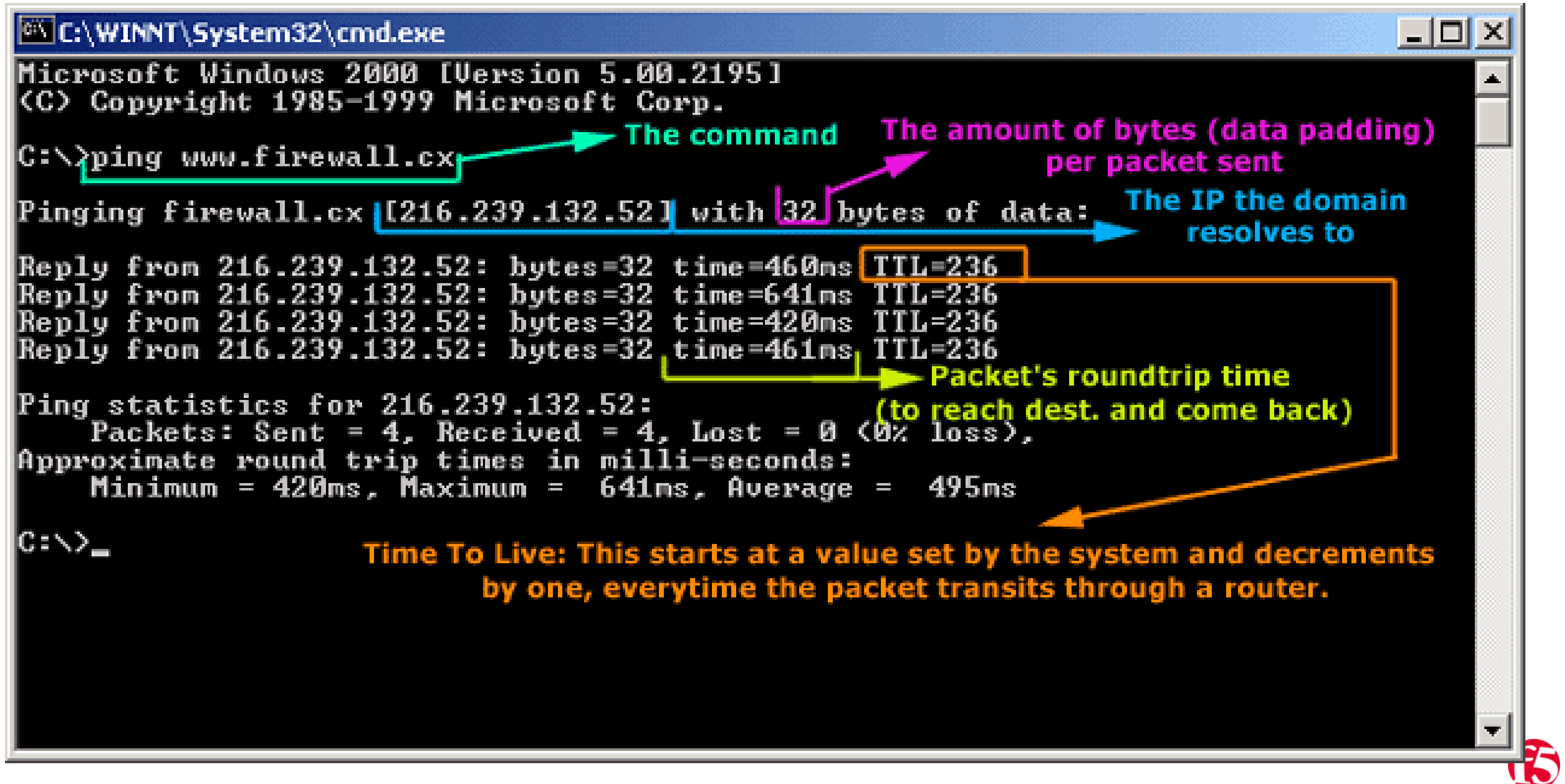
- Explain the purpose of an IP TTL
  - https://en.wikipedia.org/wiki/Keepalive



# Objective 4.01

## Explain common uses for ICMP

- Explain the purpose of ICMP echo request/reply
  - https://en.wikipedia.org/wiki/Ping_(networking_utility)
  - ICMP Tools
    - Ping
    - Traceroute



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ping www.firewall.cx

Pinging firewall.cx [216.239.132.52] with 32 bytes of data:

Reply from 216.239.132.52: bytes=32 time=460ms TTL=236
Reply from 216.239.132.52: bytes=32 time=641ms TTL=236
Reply from 216.239.132.52: bytes=32 time=420ms TTL=236
Reply from 216.239.132.52: bytes=32 time=461ms TTL=236

Ping statistics for 216.239.132.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 420ms, Maximum =  641ms, Average =  495ms

C:\>_
```

The command

The amount of bytes (data padding) per packet sent

The IP the domain resolves to

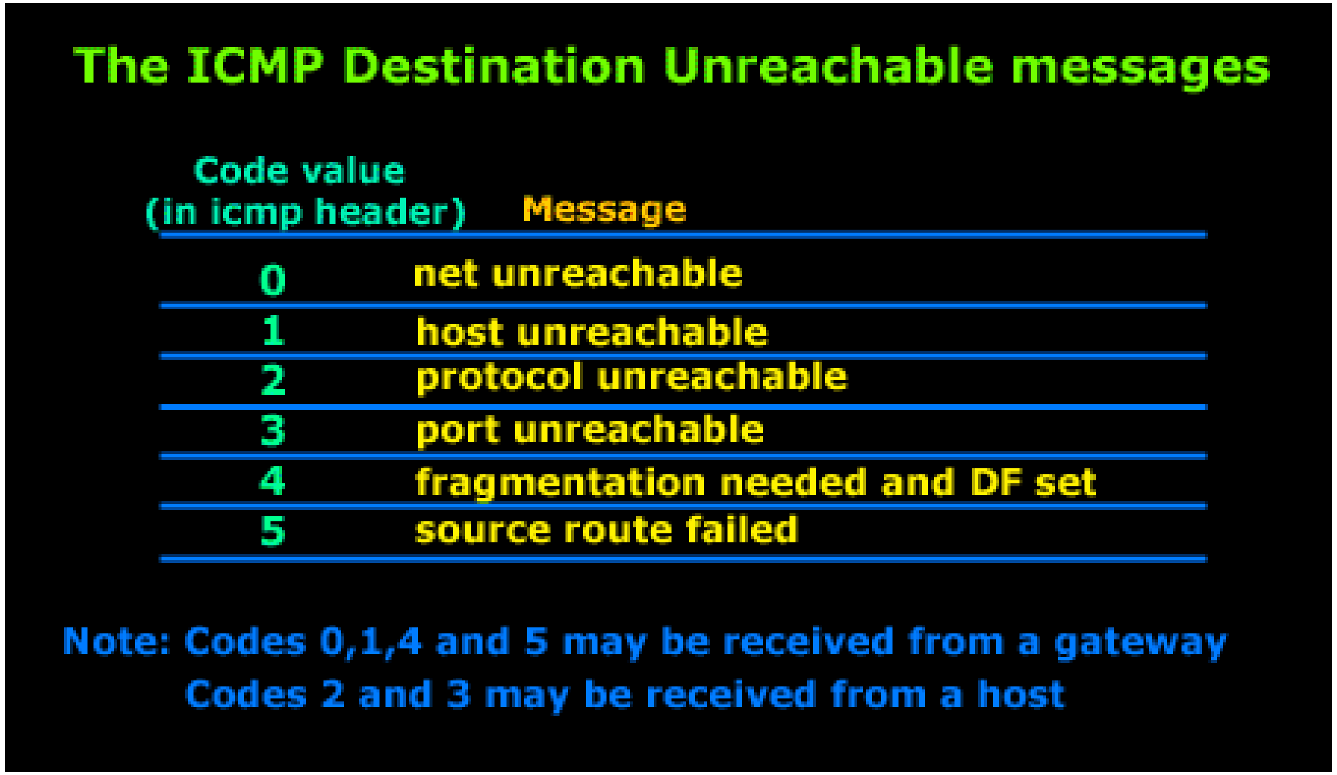
Packet's roundtrip time (to reach dest. and come back)

Time To Live: This starts at a value set by the system and decrements by one, everytime the packet transits through a router.

# Objective 4.01

Explain common uses for ICMP

- Explain reasons for ICMP unreachable
  - https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol



The ICMP Destination Unreachable messages

| Code value<br>(in icmp header) | Message |
|---|---|
| 0 | net unreachable |
| 1 | host unreachable |
| 2 | protocol unreachable |
| 3 | port unreachable |
| 4 | fragmentation needed and DF set |
| 5 | source route failed |

Note: Codes 0,1,4 and 5 may be received from a gateway
Codes 2 and 3 may be received from a host

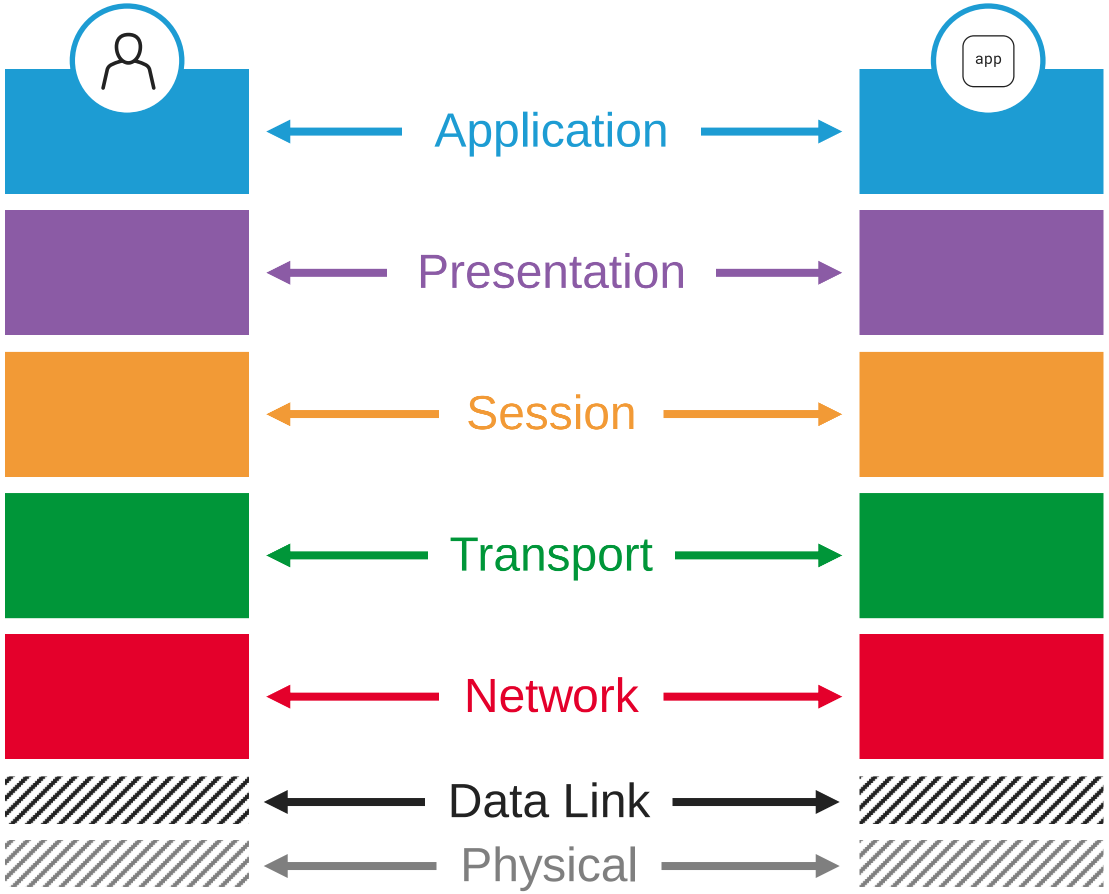
# Objective 4.02

## MAP FUNCTIONALITY TO OSI MODEL

- Identify the layer for a MAC address
- Identify the layer for a UDP/TCP port
- Identify the layer for an IP address
- Identify the layer for applications

# 7 Standard Layers in the OSI Model

With examples at each layer



Application

Presentation

Session

Transport

Network

Data Link

Physical

L7. HTTP (web), SMTP (email)

L6. JSON, XML, MIME

L5. NetBIOS, RPC

L4. TCP (data), UDP (streaming)

L3. IP (IPv4), IPv6, ping

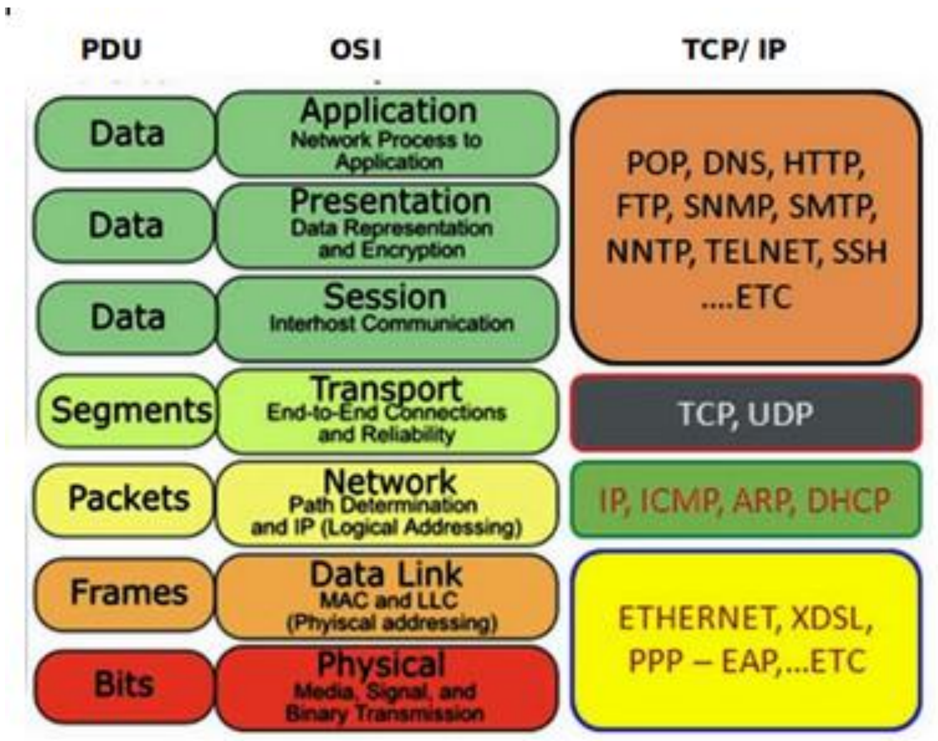
L2. WiFi, Ethernet

L1. Cat6 cable, fiber optic, radio

# Protocol Data Unit (PDU)

**COMMIT TO MEMORY!:** A PDU IS COMPOSED OF PROTOCOL-SPECIFIC CONTROL INFORMATION AND USER DATA

- **OSI model**
- Protocol data units of the OSI model are:
- The Layer 4: transport layer PDU is the segment
- The Layer 3: network layer PDU is the packet.
- The Layer 2: data link layer PDU is the frame.
- The Layer 1: physical layer PDU is the bit



| PDU | OSI | TCP/ IP |
|---|---|---|
| Data | Application<br>Network Process to Application | POP, DNS, HTTP, FTP, SNMP, SMTP, NNTP, TELNET, SSH ....ETC |
| Data | Presentation<br>Data Representation and Encryption | |
| Data | Session<br>Interhost Communication | |
| Segments | Transport<br>End-to-End Connections and Reliability | TCP, UDP |
| Packets | Network<br>Path Determination and IP (Logical Addressing) | IP, ICMP, ARP, DHCP |
| Frames | Data Link<br>MAC and LLC (Phyiscal addressing) | ETHERNET, XDSL, PPP – EAP,...ETC |
| Bits | Physical<br>Media, Signal, and Binary Transmission | |

# Objective 4.03

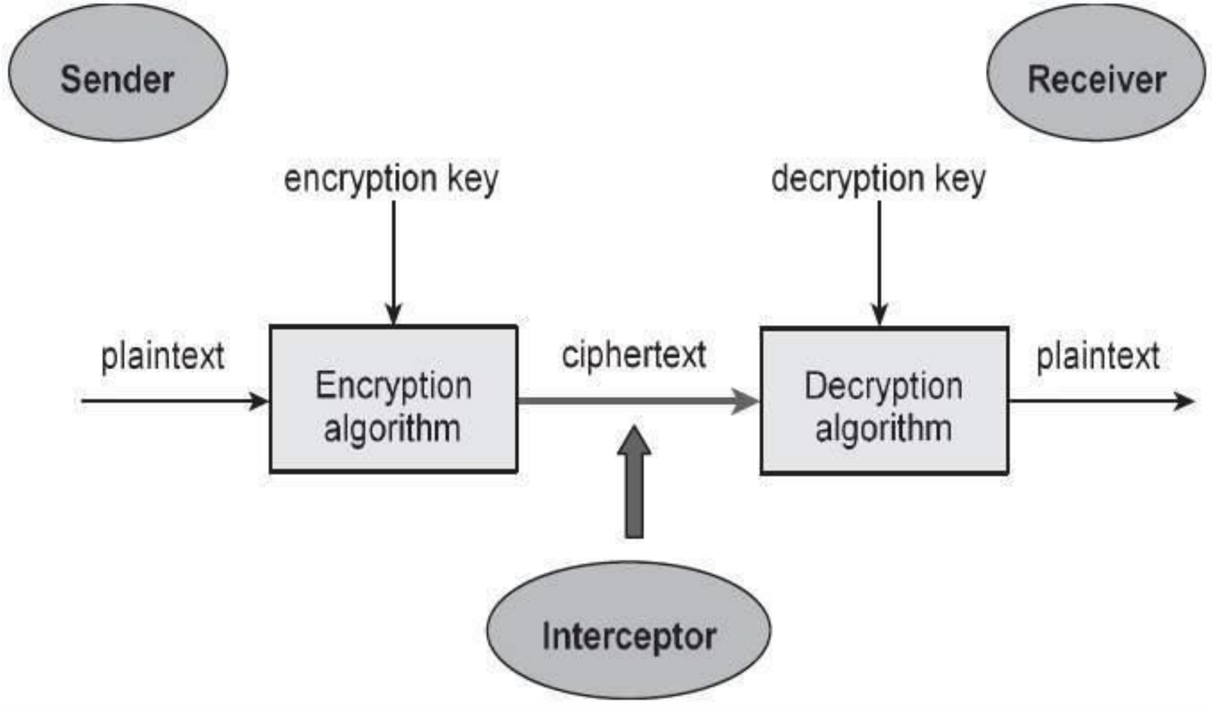
## EXPLAIN USE OF TLS/SSL

- Explain the purpose of TLS/SSL certificates (self signed vs CA signed)
- Explain the rationale for using TLS/SSL

# Objective 4.03

Explain use of TLS/SSL

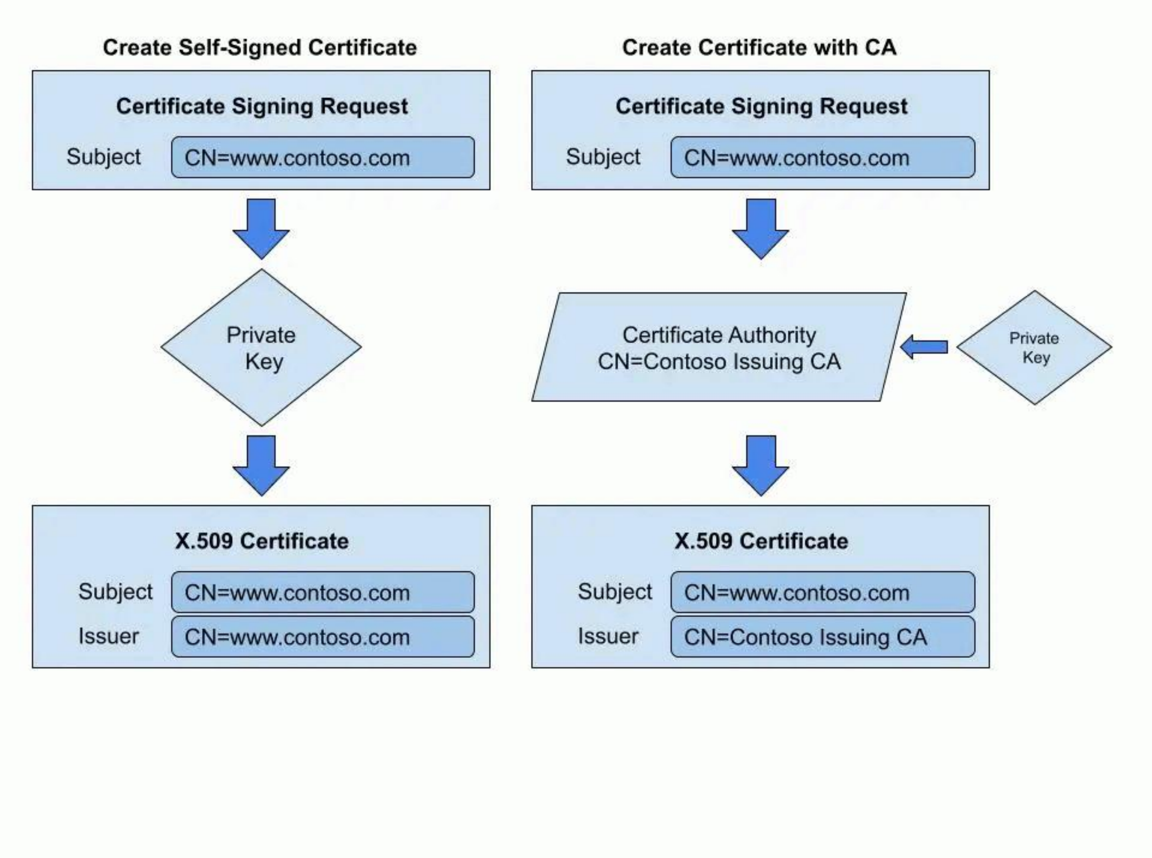
- Explain the rationale for using TLS/SSL



# Objective 4.03

Explain use of TLS/SSL

- Explain the purpose of TLS/SSL certificates (self signed vs CA signed)



# Objective 4.04

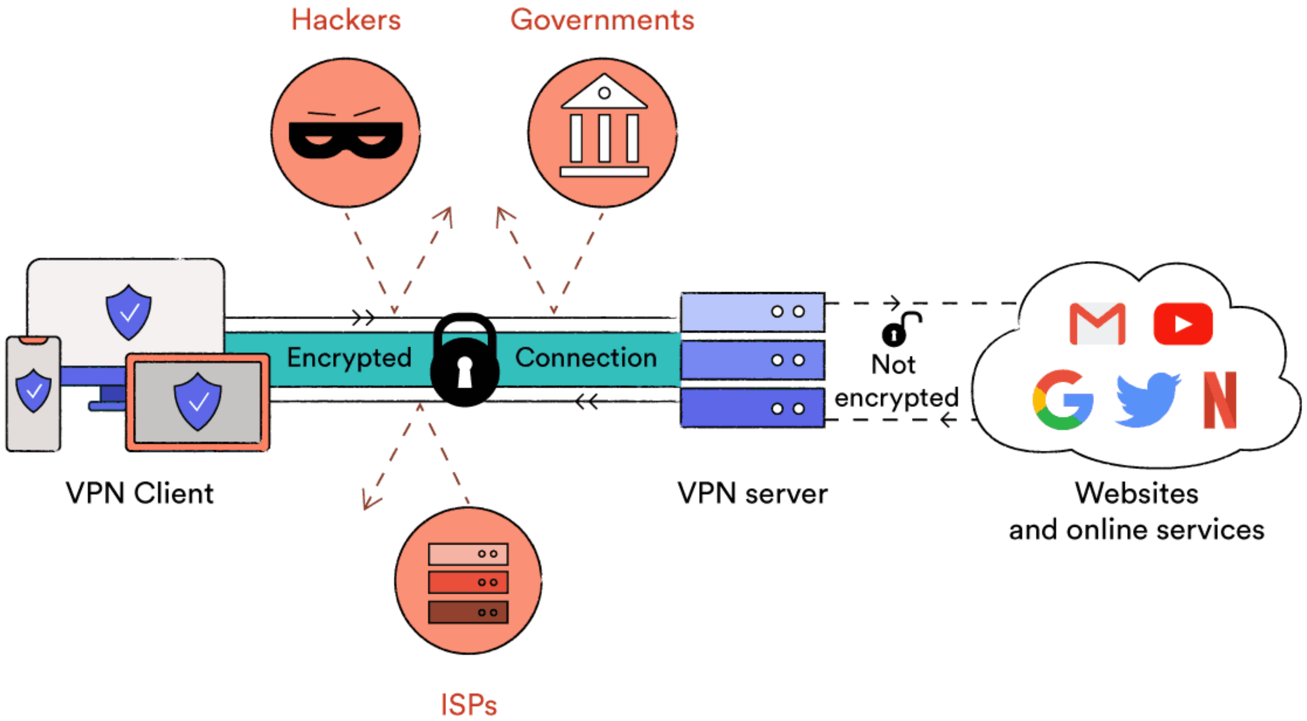
## EXPLAIN THE FUNCTION OF A VPN

- Explain the rationale for using VPN (privacy, encryption, anonymity)
- Identify valid uses for VPN

# Objective 4.04

Explain the function of a VPN

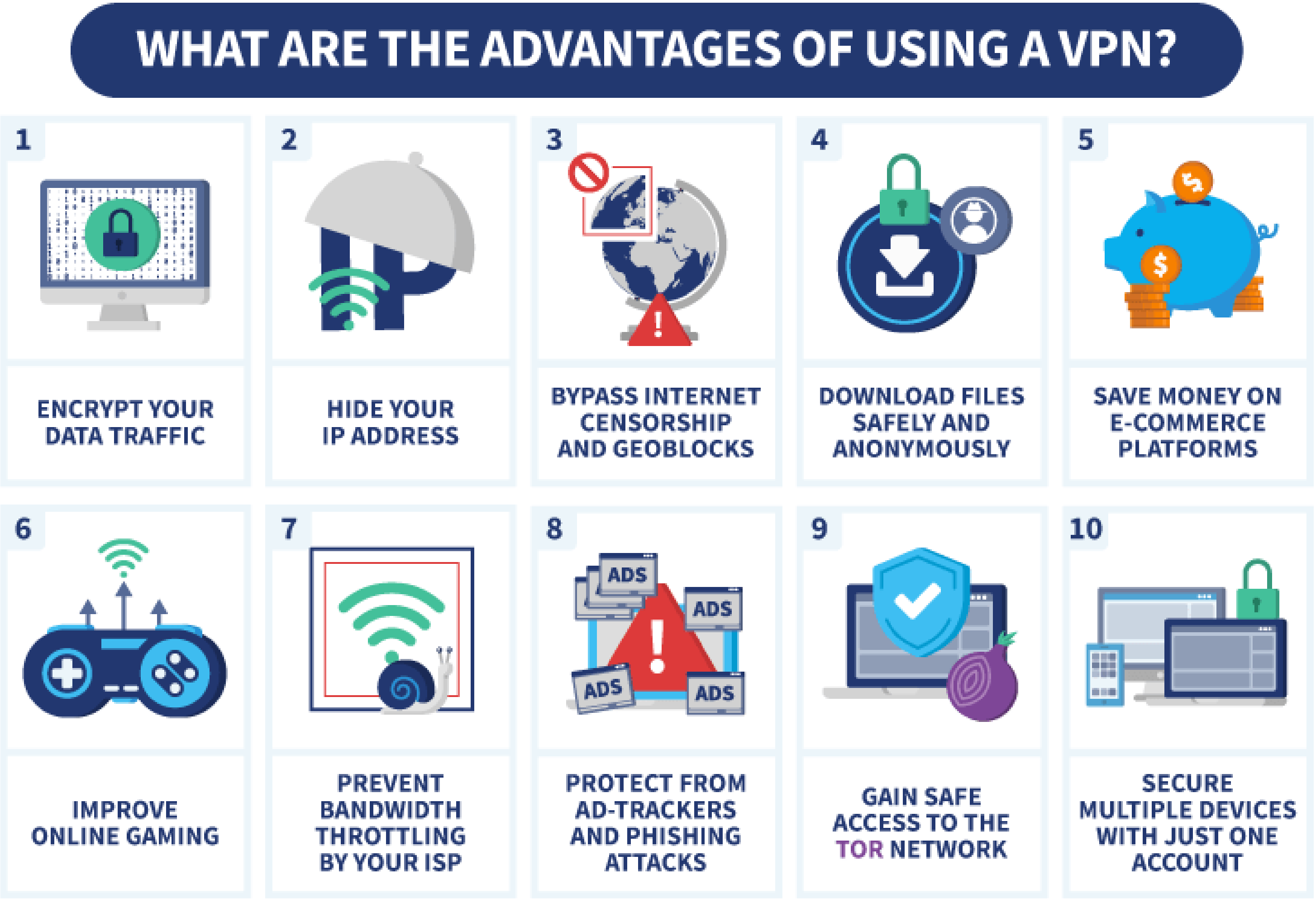
- **Explain the function of a VPN**
  - https://en.wikipedia.org/wiki/Virtual_private_network



# Objective 4.04

Explain the function of a VPN

- **Explain the rationale for using VPN (privacy, encryption, anonymity)**



WHAT ARE THE ADVANTAGES OF USING A VPN?

1 ENCRYPT YOUR DATA TRAFFIC

2 HIDE YOUR IP ADDRESS

3 BYPASS INTERNET CENSORSHIP AND GEOBLOCKS

4 DOWNLOAD FILES SAFELY AND ANONYMOUSLY

5 SAVE MONEY ON E-COMMERCE PLATFORMS

6 IMPROVE ONLINE GAMING

7 PREVENT BANDWIDTH THROTTLING BY YOUR ISP

8 PROTECT FROM AD-TRACKERS AND PHISHING ATTACKS

9 GAIN SAFE ACCESS TO THE TOR NETWORK

10 SECURE MULTIPLE DEVICES WITH JUST ONE ACCOUNT

# Objective 4.05

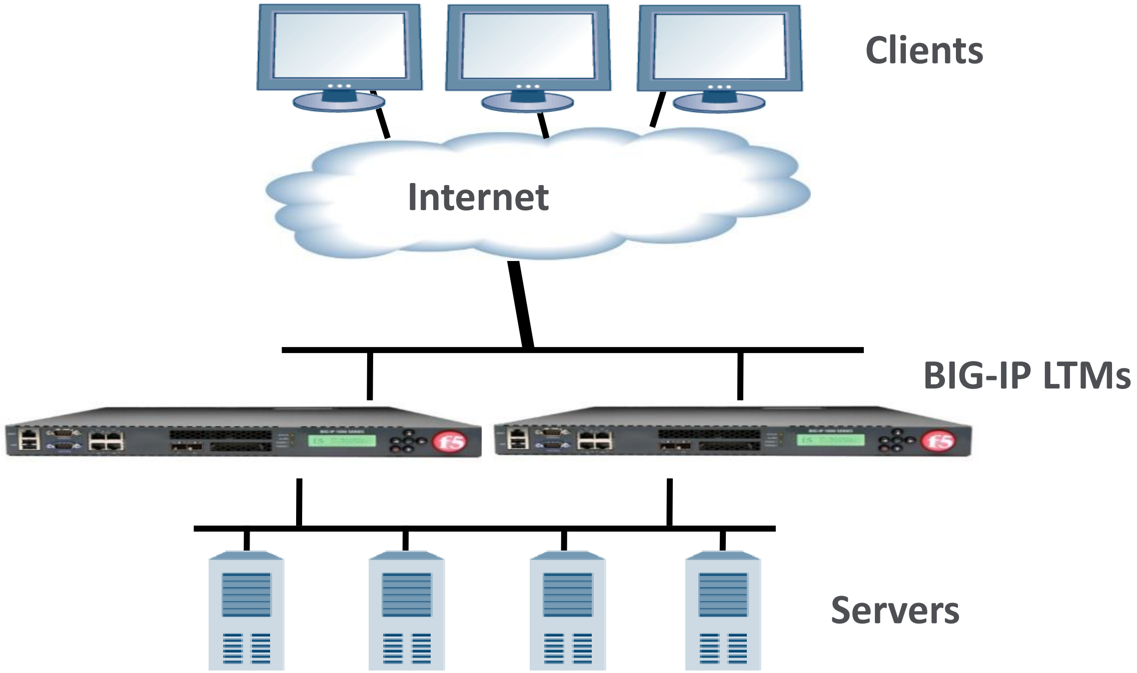
## EXPLAIN HIGH AVAILABILITY

- Explain methods of providing HA integrity
- Explain methods of providing HA
- Explain advantages of HA

# Objective 4.05

- Explain high availability (HA) concepts

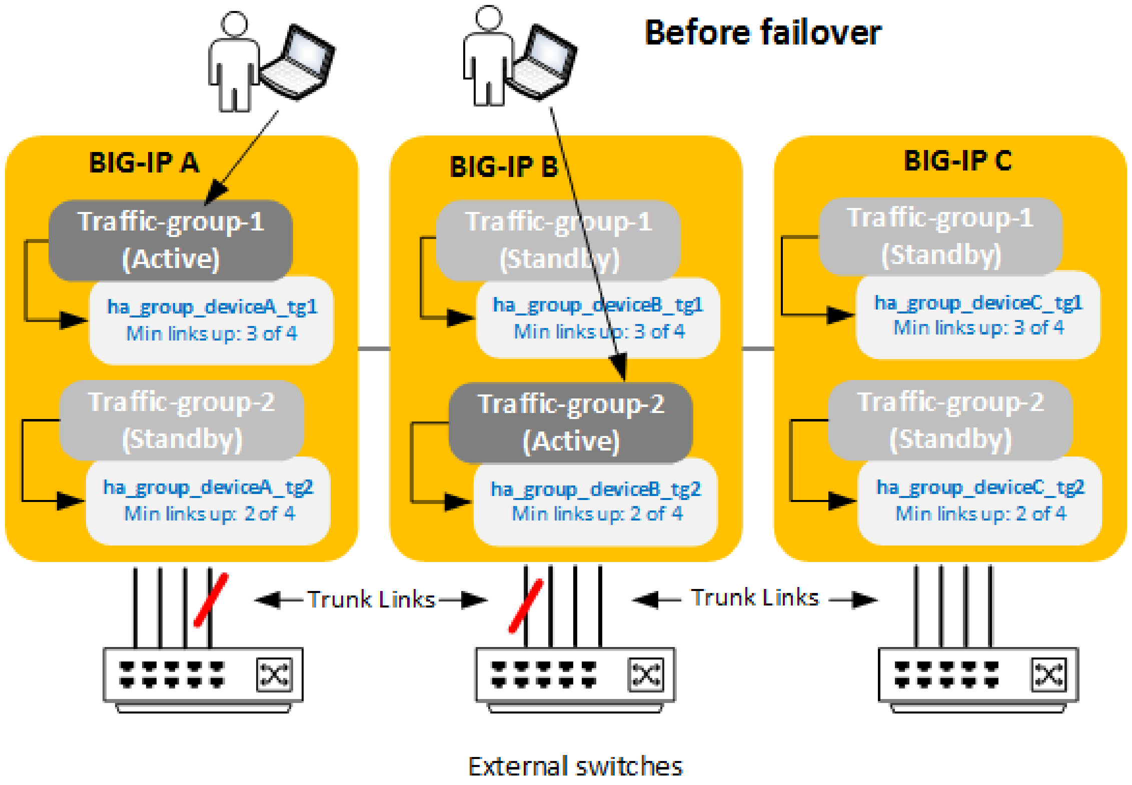
## Explain advantages of HA



# Objective 4.05

## Explain high availability (HA) concepts

- **Explain methods of providing HA**
  - Active/Active
  - Active/Passive
  - Device service clustering



Before failover
BIG-IP A
Traffic-group-1 (Active)
ha_group_deviceA_tg1 Min links up: 3 of 4
Traffic-group-2 (Standby)
ha_group_deviceA_tg2 Min links up: 2 of 4
BIG-IP B
Traffic-group-1 (Standby)
ha_group_deviceB_tg1 Min links up: 3 of 4
Traffic-group-2 (Active)
ha_group_deviceB_tg2 Min links up: 2 of 4
BIG-IP C
Traffic-group-1 (Standby)
ha_group_deviceC_tg1 Min links up: 3 of 4
Traffic-group-2 (Standby)
ha_group_deviceC_tg2 Min links up: 2 of 4
Trunk Links
Trunk Links
External switches

# Objective 4.05

## EXPLAIN HIGH AVAILABILITY

- **Explain methods of providing HA integrity**
  - **System Fail-safe**: monitors various hardware components, as well as the heartbeat of various system services
  - **VLAN Fail-safe**: monitors network traffic going through a specified VLAN
  - **Gateway Fail-safe**: monitors traffic between an active BIG-IP® system in a device group and a pool containing a gateway router

# Objective 4.06

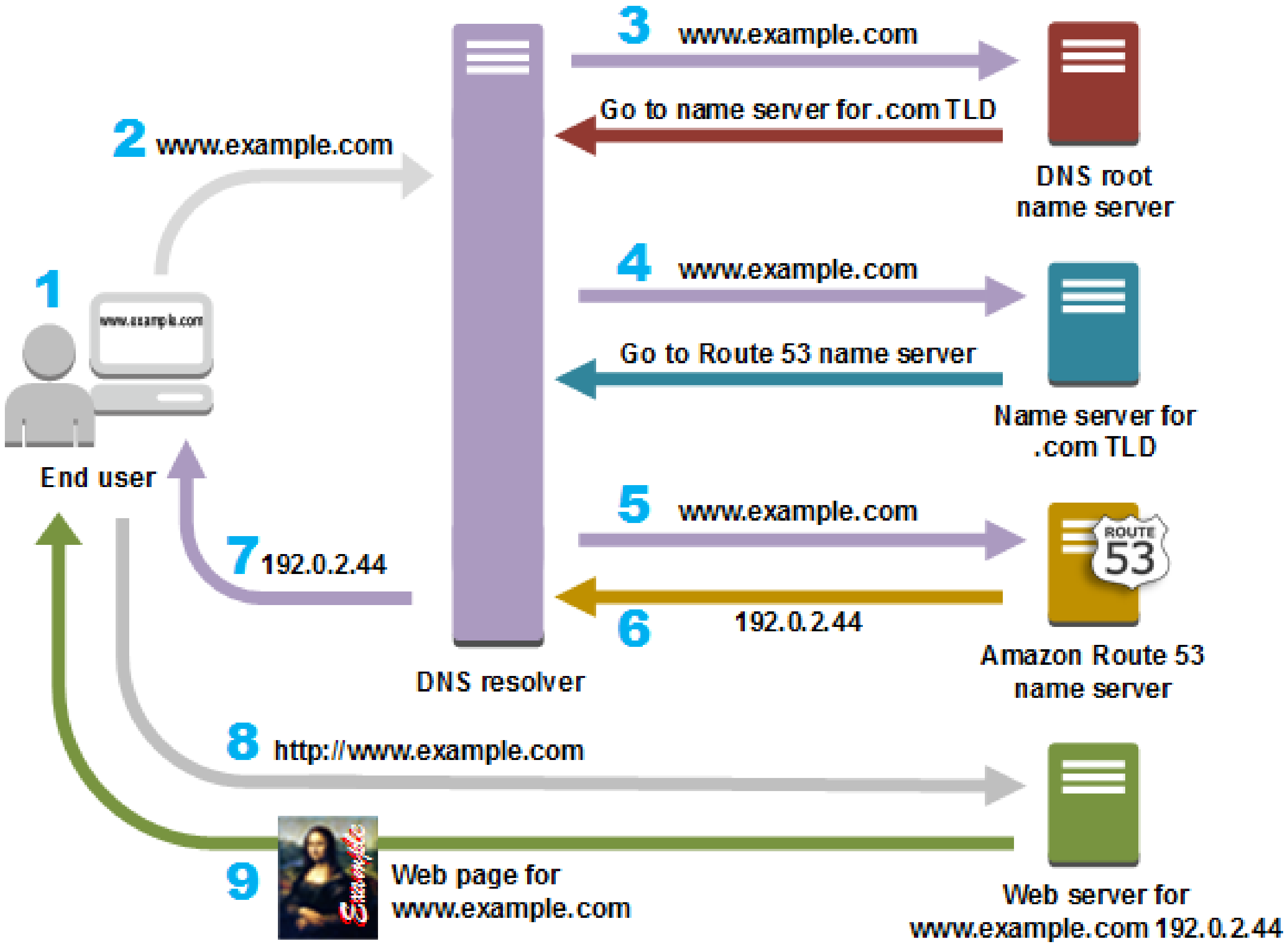
## EXPLAIN HIGH AVAILABILITY

- Explain the purpose of DNS
- Given a list of tools, select the appropriate tool to confirm DNS resolution is successful for a host name
- Explain what syslog is
- Explain the purpose of NTP
- Explain SNMP as it pertains to ADC element monitoring

# Objective 4.06

Explain reasons for support services (DNS, NTP, syslog, SNMP, etc)

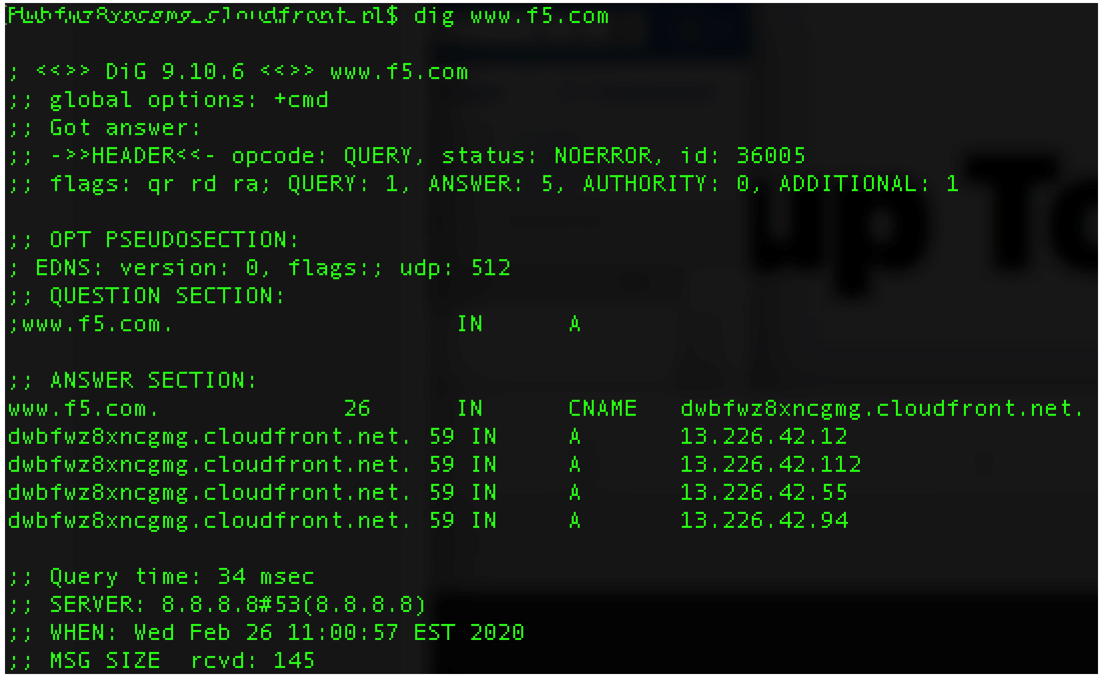
- Explain the purpose of DNS



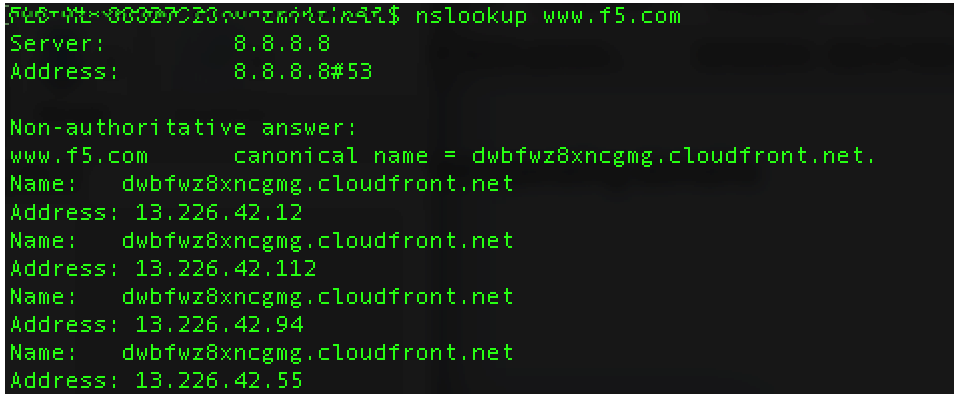
# Objective 4.06

Explain reasons for support services (DNS, NTP, syslog, SNMP, etc)

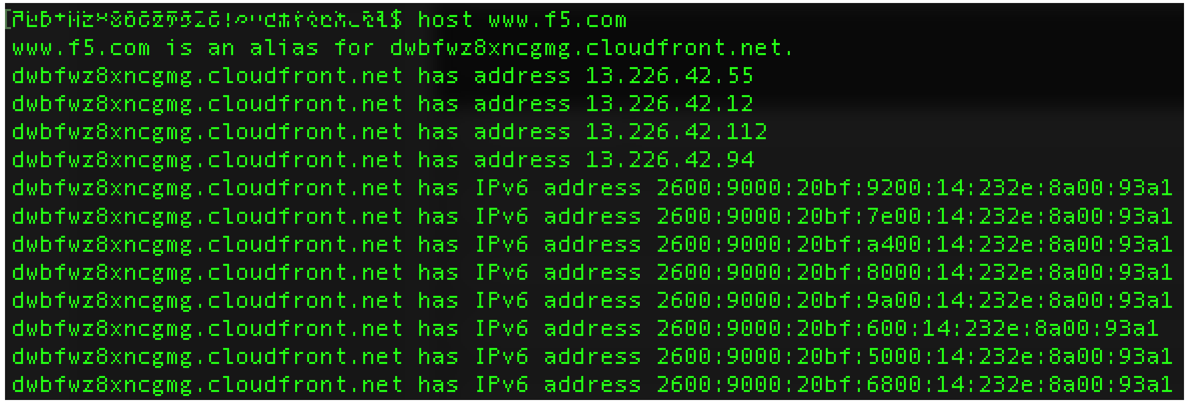
- Given a list of tools, select the appropriate tool to confirm DNS resolution is successful for a host name
- https://blog.dnsimple.com/2015/02/top-dns-lookup-tools/
- DNS Tools - “nsLookup”, “dig” and “host”



```
[illegible]$ dig www.f5.com

; <<>> DiG 9.10.6 <<>> www.f5.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36005
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.f5.com.                    IN      A

;; ANSWER SECTION:
www.f5.com.             26      IN      CNAME   dwbfwz8xncgmg.cloudfront.net.
dwbfwz8xncgmg.cloudfront.net. 59 IN     A       13.226.42.12
dwbfwz8xncgmg.cloudfront.net. 59 IN     A       13.226.42.112
dwbfwz8xncgmg.cloudfront.net. 59 IN     A       13.226.42.55
dwbfwz8xncgmg.cloudfront.net. 59 IN     A       13.226.42.94

;; Query time: 34 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Feb 26 11:00:57 EST 2020
;; MSG SIZE  rcvd: 145
```



```
[illegible]$ nslookup www.f5.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.f5.com      canonical name = dwbfwz8xncgmg.cloudfront.net.
Name:   dwbfwz8xncgmg.cloudfront.net
Address: 13.226.42.12
Name:   dwbfwz8xncgmg.cloudfront.net
Address: 13.226.42.112
Name:   dwbfwz8xncgmg.cloudfront.net
Address: 13.226.42.94
Name:   dwbfwz8xncgmg.cloudfront.net
Address: 13.226.42.55
```

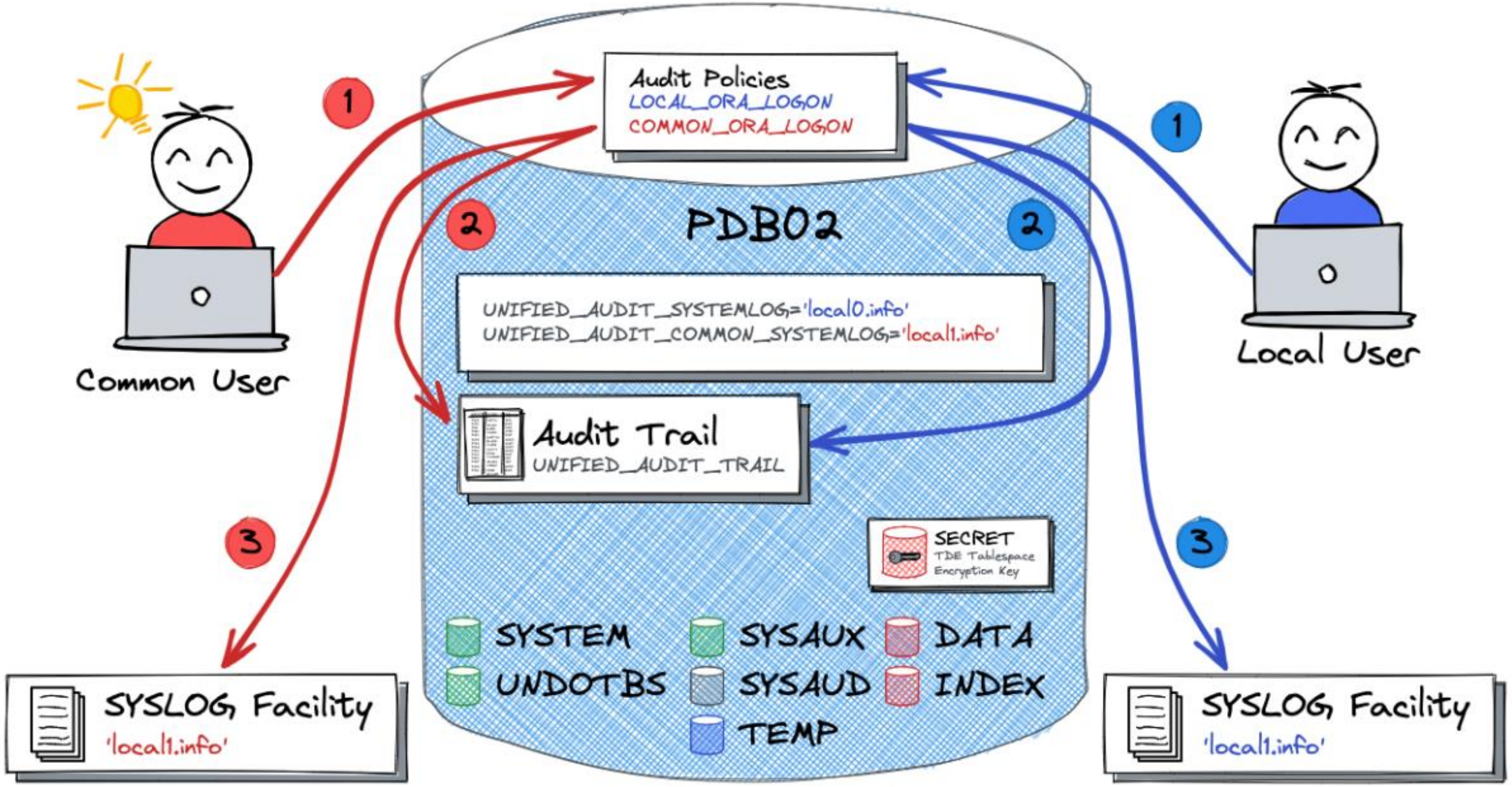


```
[illegible]$ host www.f5.com
www.f5.com is an alias for dwbfwz8xncgmg.cloudfront.net.
dwbfwz8xncgmg.cloudfront.net has address 13.226.42.55
dwbfwz8xncgmg.cloudfront.net has address 13.226.42.12
dwbfwz8xncgmg.cloudfront.net has address 13.226.42.112
dwbfwz8xncgmg.cloudfront.net has address 13.226.42.94
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:9200:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:7e00:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:a400:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:8000:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:9a00:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:600:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:5000:14:232e:8a00:93a1
dwbfwz8xncgmg.cloudfront.net has IPv6 address 2600:9000:20bf:6800:14:232e:8a00:93a1
```

# Objective 4.06

## Explain reasons for support services (DNS, NTP, syslog, SNMP, etc)

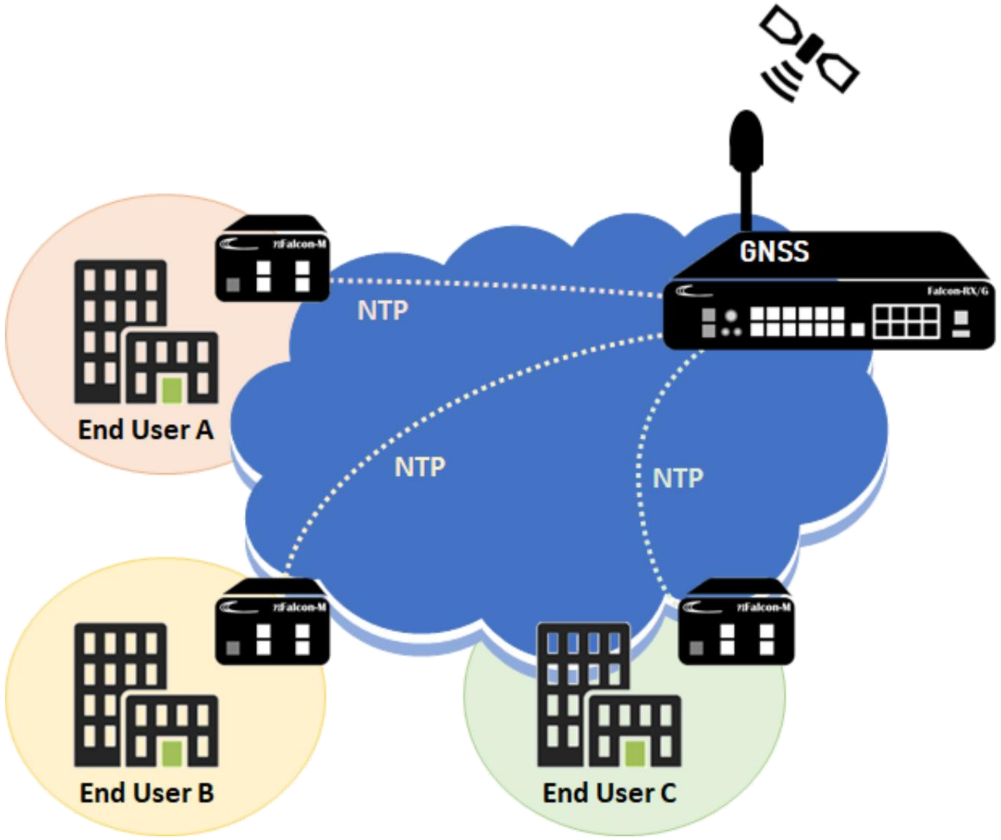
- Explain what syslog?



# Objective 4.06

Network Time Protocol

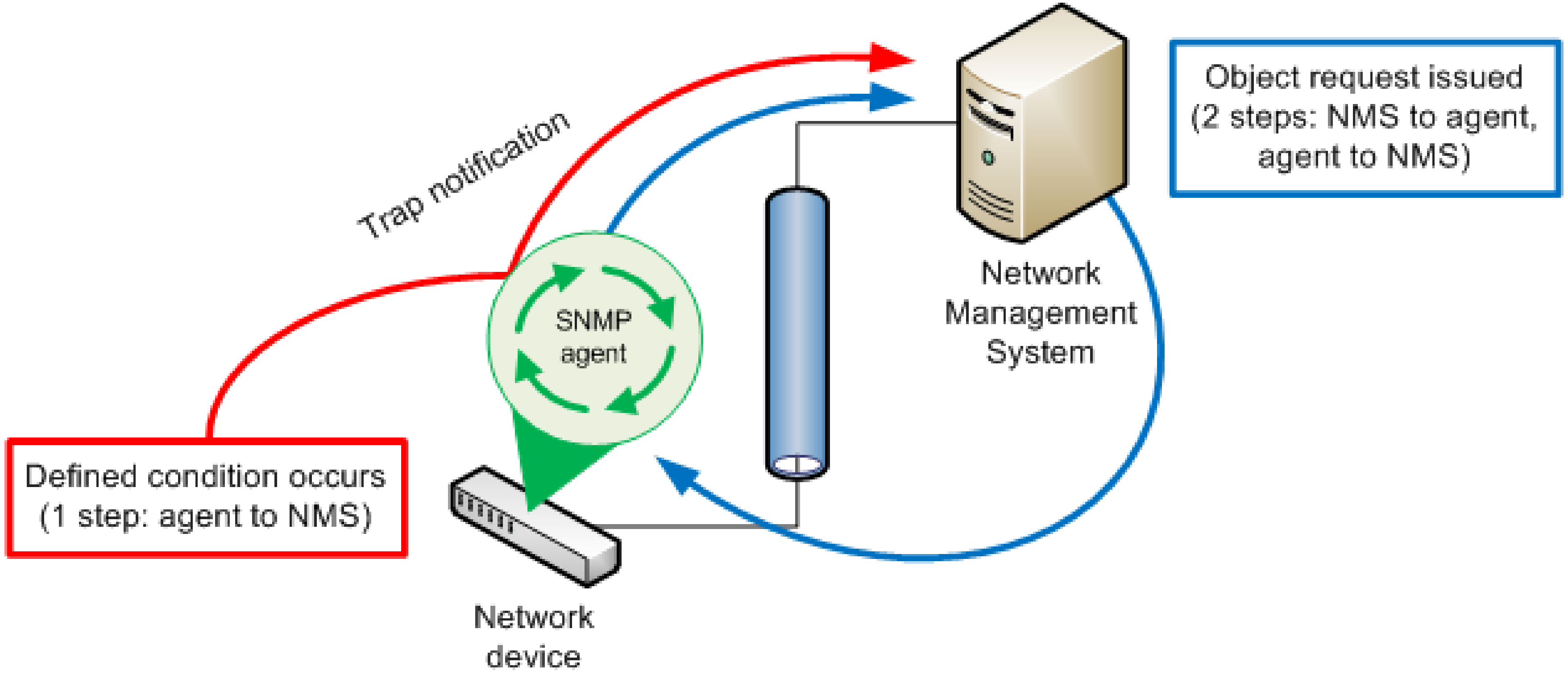
- Explain the purpose of NTP
  - https://en.wikipedia.org/wiki/Network_Time_Protocol



# Objective 4.06

Explain reasons for support services (DNS, NTP, syslog, SNMP, etc)

- Explain SNMP as it pertains to ADC element monitoring



Object request issued (2 steps: NMS to agent, agent to NMS)

Defined condition occurs (1 step: agent to NMS)

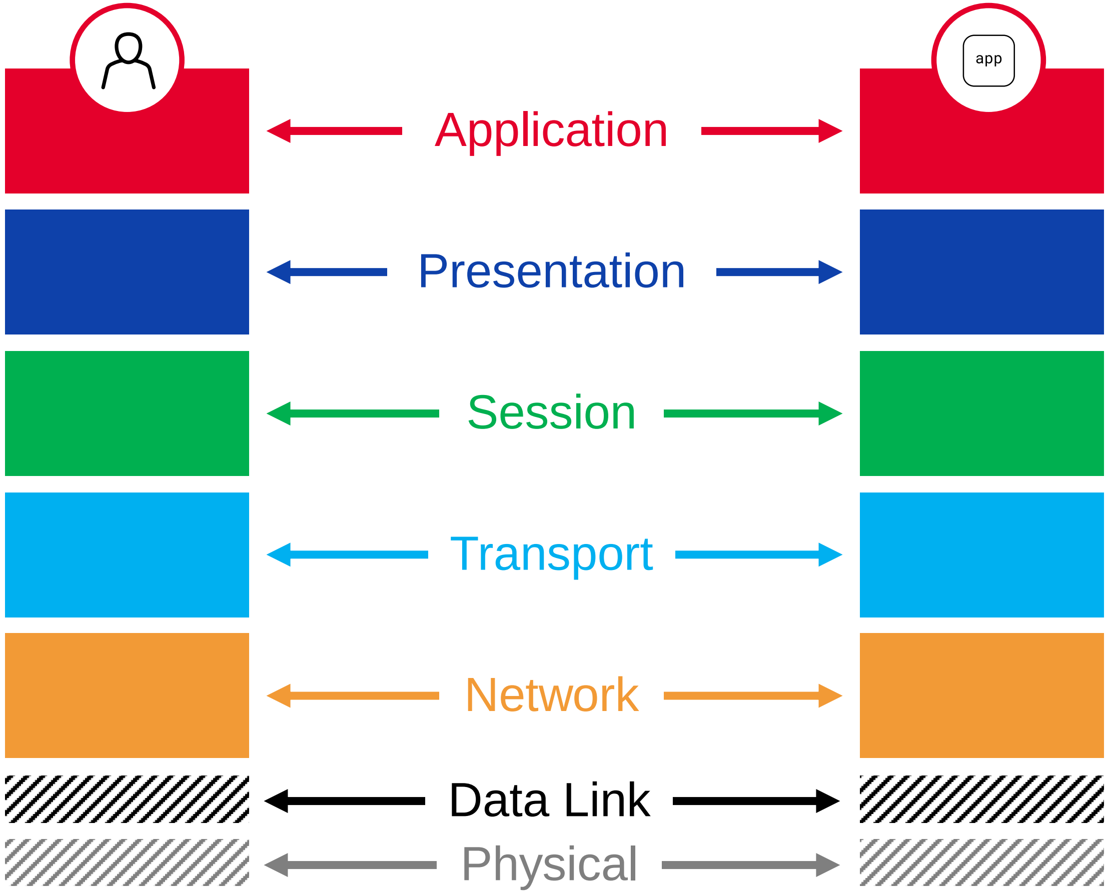
# Section 1: Configuration

# Agenda Section 1:

- Open Systems Interconnect (OSI) Model intro
- Virtual Local Area Networks (VLANs) & how to configure
- Self IPs
- Routers – Firewalls – Switches
- IP address classes and subnetting
- Network Address Translation (NAT) & Dynamic Host configuration Protocol (DHCP)
- Address Resolution Protocol (ARP)
- Routes and Routing Tables
- Application Delivery Controller (ADC)

# 7 Standard Layers in the OSI Model

With examples at each layer



L7. HTTP (web), SMTP (email)

L6. JSON, XML, MIME

L5. NetBIOS, RPC

L4. TCP (data), UDP (streaming)

L3. IP (IPv4), IPv6, ping

L2. Wi-Fi, Ethernet

L1. Cat6 cable, fiber optic, radio

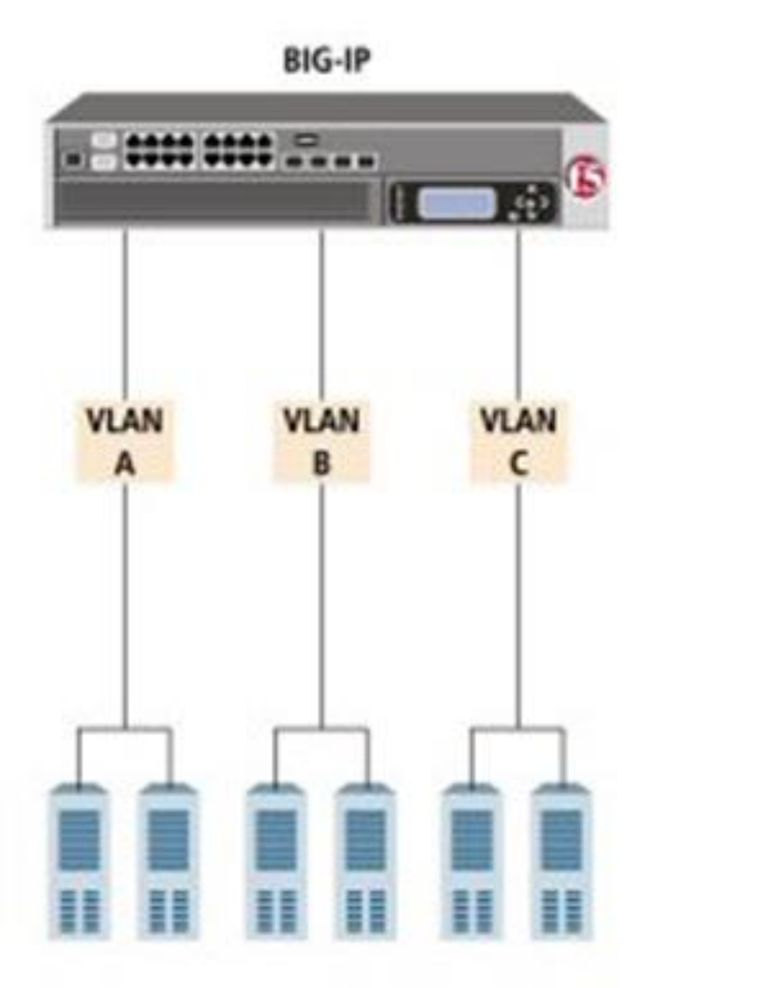
# VLANs

**DEFINITION:**

A Virtual Local Area Network is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI Layer 2).

**WHY use VLANs?**

- Reduces the size of broadcast domain – increases network performance
- Reduce network maintenance tasks
- Group endpoints by functional roles even if physically dispersed
- Improves security by separating traffic via network segmentation



# Tagged vs Untagged Interfaces

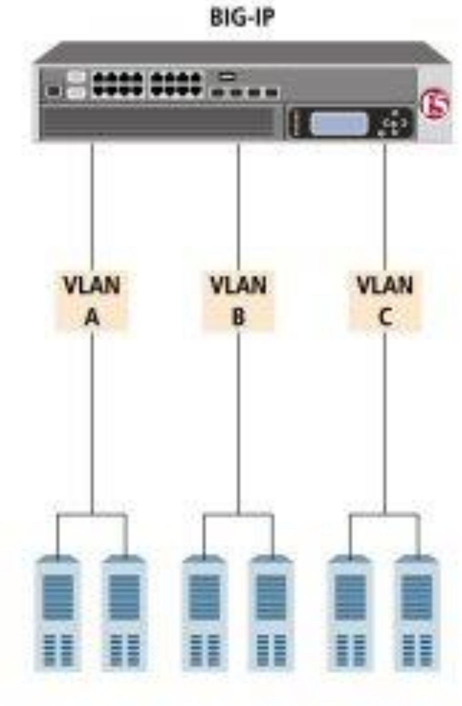
**Untagged interfaces**

You can create a VLAN and assign interfaces to the VLAN as untagged interfaces. When you assign interfaces as *untagged interfaces*, you cannot associate other VLANs with those interfaces. This limits the interface to accepting traffic only from that VLAN, instead of from multiple VLANs.

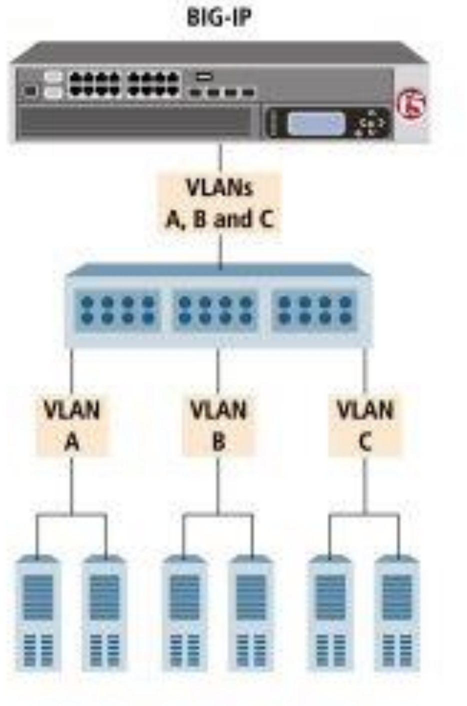
**Tagged interfaces**

If you want to give an interface the ability to accept and receive traffic for multiple vlans, you add the same interface to each VLAN as a tagged interface. When you assign interfaces as *tagged interfaces*, you can associate multiple VLANs with those interfaces.

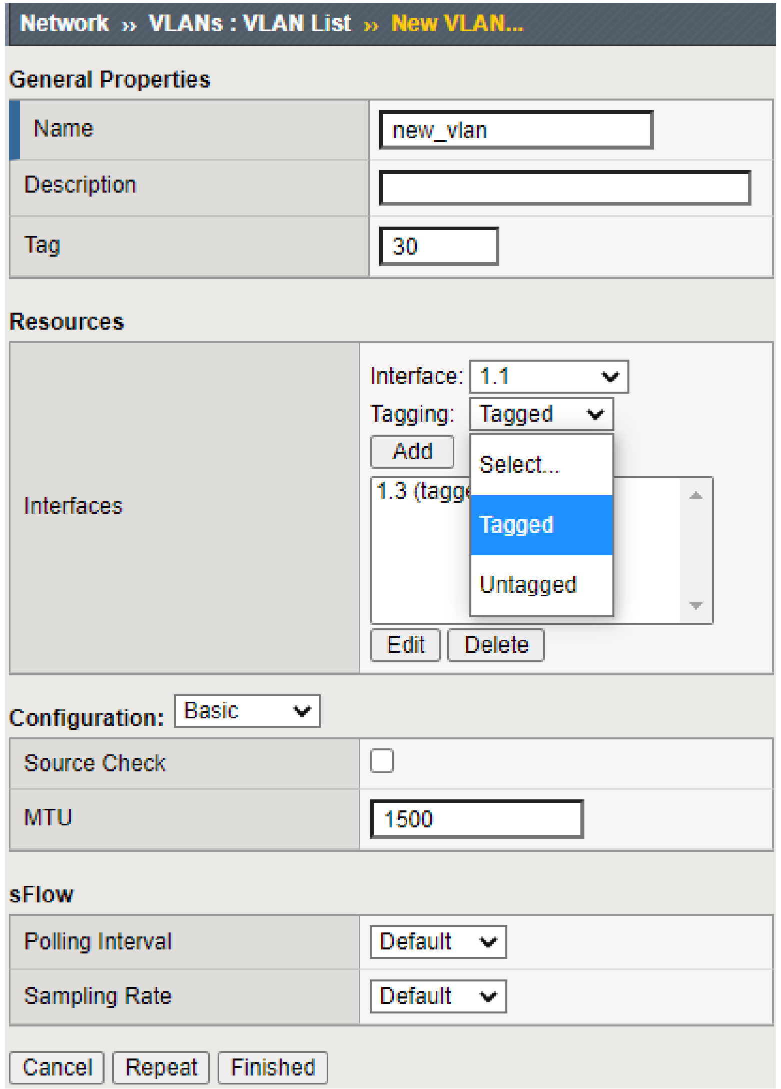
**Untagged Interfaces**



**Tagged Interfaces**



# Tagged vs Untagged Interfaces



General Properties

| | |
|---|---|
| Name | new_vlan |
| Description | |
| Tag | 30 |

Resources

| | |
|---|---|
| Interfaces | Interface: 1.1<br>Tagging: Tagged<br>1.3 (tagge |

Configuration: Basic

| | |
|---|---|
| Source Check | □ |
| MTU | 1500 |

sFlow

| | |
|---|---|
| Polling Interval | Default |
| Sampling Rate | Default |

[Manual Chapter : VLANs VLAN Groups and VXLAN]

If you wish to have more than one VLAN over the same physical interface or trunk

Place interfaces and trunks into the Untagged or Tagged boxes

**Untagged** interfaces do not require a Tag be entered

- The BIG-IP will assign a Tag to logically separate internal traffic

**Tagged** interfaces run **802.1q VLAN** tagging

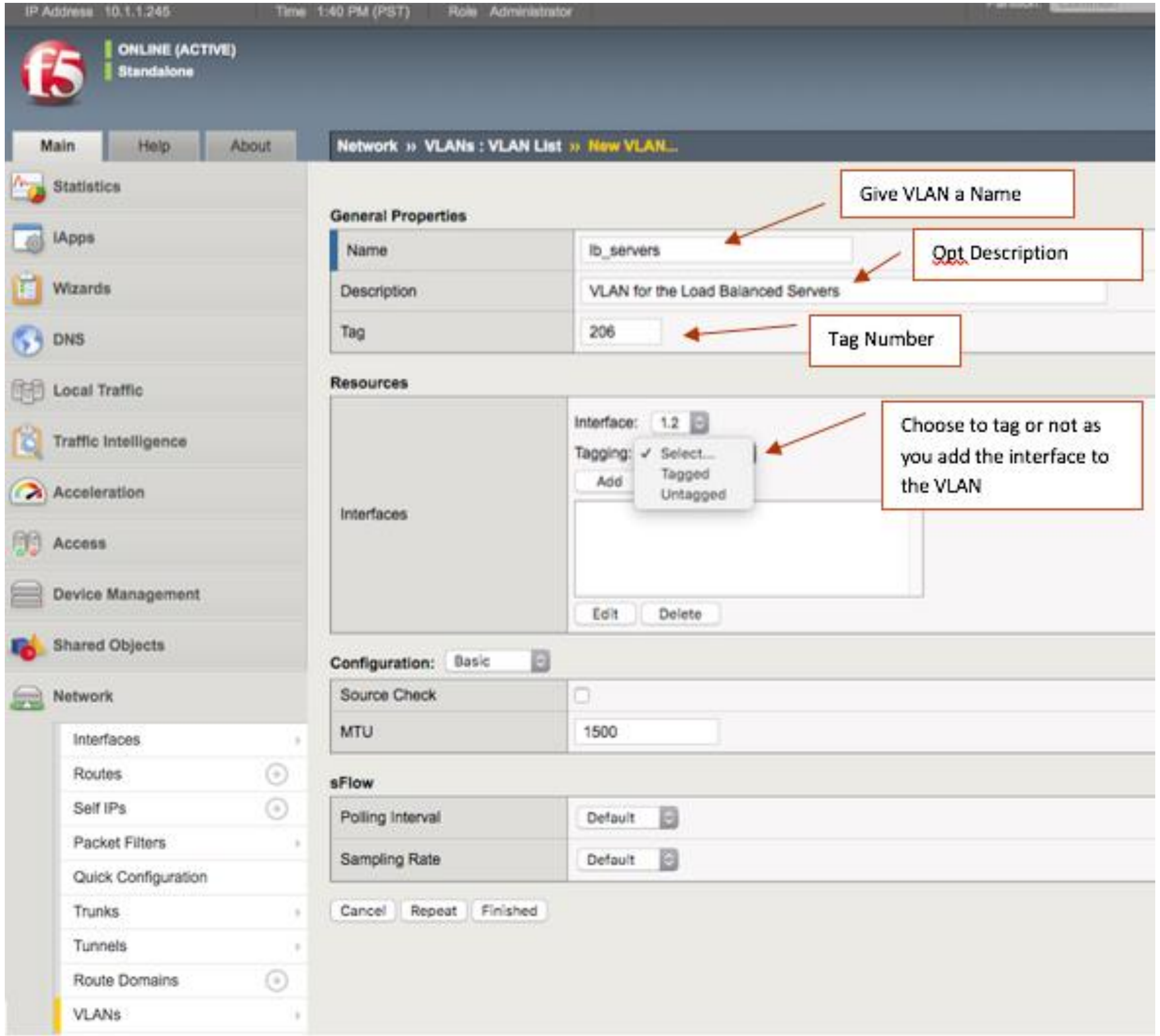
- You need to manually enter the tag

# Objective 1.01

Given a set of requirements, configure VLANs

Assign a numeric tag to the VLAN if required

- Assigning a tag number to the VLAN
- Associate an interface as tagged or untagged



Network » VLANs : VLAN List » New VLAN...

**General Properties**

| | |
|---|---|
| Name | lb_servers |
| Description | VLAN for the Load Balanced Servers |
| Tag | 206 |

Give VLAN a Name

Opt Description

Tag Number

**Resources**

Interfaces

Interface: 1.2

Tagging: ✓ Select...<br>Tagged<br>Untagged

Add

Edit Delete

Choose to tag or not as you add the interface to the VLAN

**Configuration:** Basic

| | |
|---|---|
| Source Check | ☐ |
| MTU | 1500 |

**sFlow**

| | |
|---|---|
| Polling Interval | Default |
| Sampling Rate | Default |

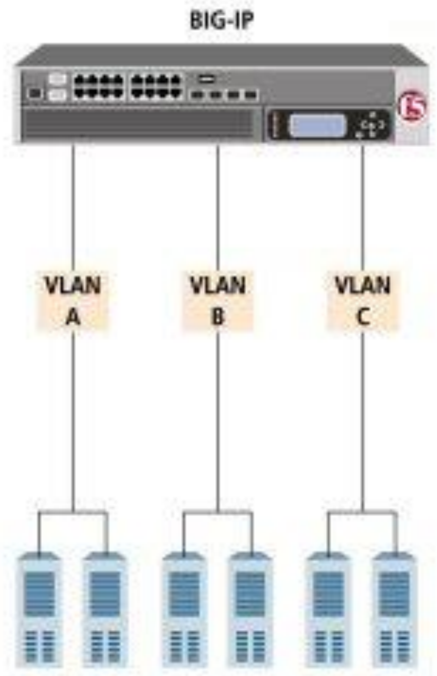
Cancel Repeat Finished

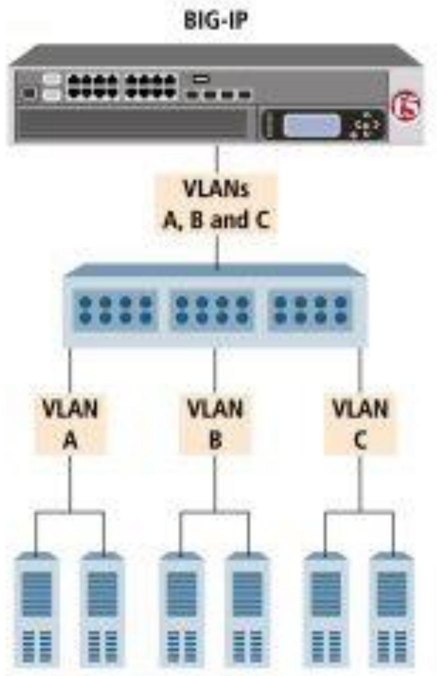
# Objective 1.01

Given a set of requirements, configure VLANs

- **F5 VLAN Tagging** = Cisco Trunking – Allowing interface to carry more than 1 VLAN
- **F5 Trunk** = Cisco Port Channel – Grouping interfaces to carry data
- **Double Tagging** *(Q-in-Q This functionality is rarely used in Enterprise architectural design)*

[https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0/vlans-vlan-groups-and-vxlan.html](https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0/vlans-vlan-groups-and-vxlan.html)



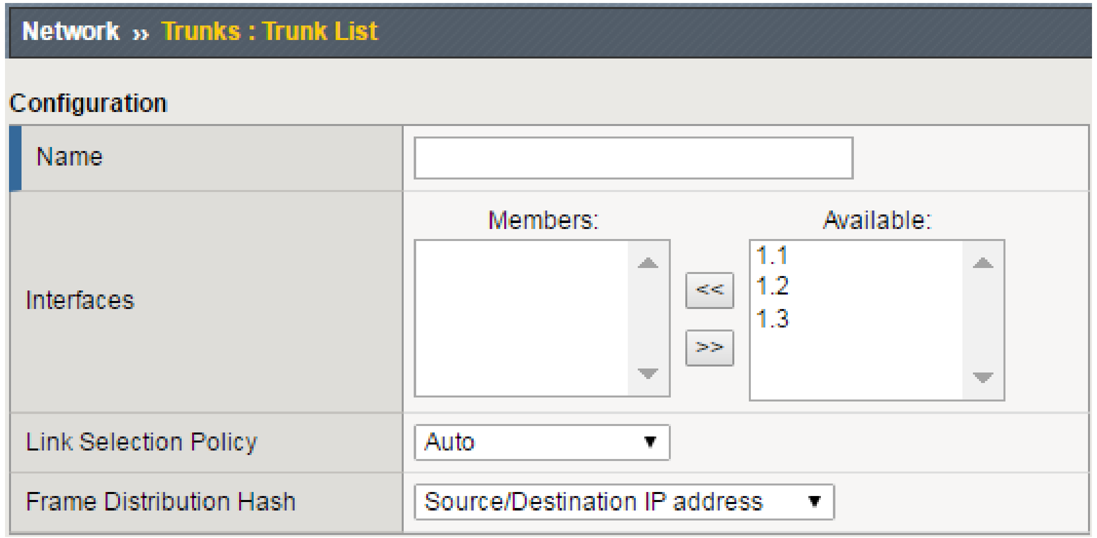


# BIG-IP Trunks

## BIG-IPS ACCEPT BOTH LACP (DEFAULT) AND ETHERCHANNEL LINK AGGREGATION

- With BIG-IP trunking you can set up **LACP 802.3ad (default)** or EtherChannel (Cisco link aggregation, support PAgP)
- Interfaces must be untagged to be added to a trunk
  - **IMPORTANT:** A BIG-IP trunk is ***not equivalent*** to a Cisco trunk which is VLAN tagging
    - Cisco terminology uses Port Channel for link aggregation

A trunk is created from the **Network >> Trunks**

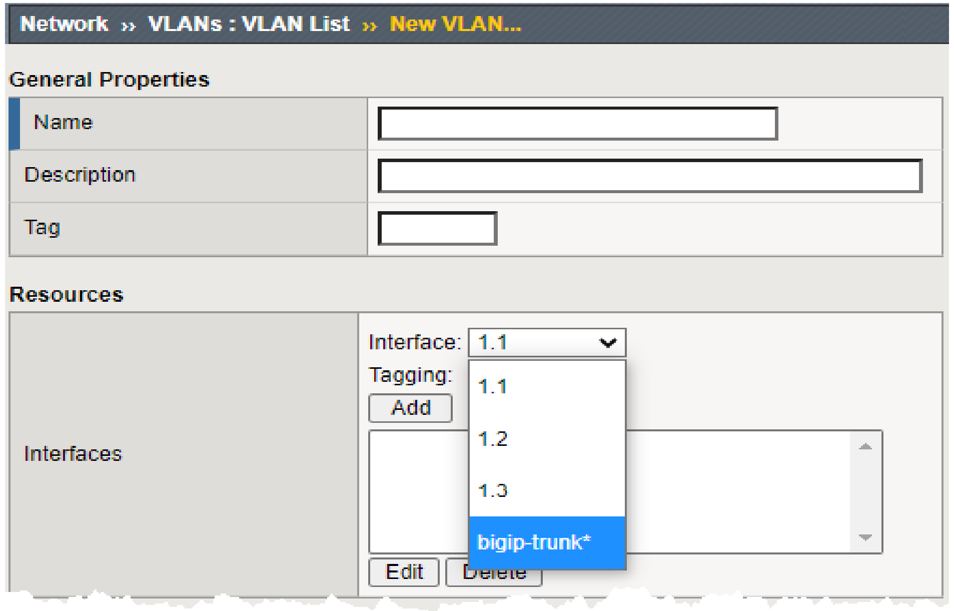


Network » Trunks : Trunk List

Configuration

| | |
|---|---|
| Name | |
| Interfaces | Members: <br> << <br> >> <br> Available: 1.1 1.2 1.3 |
| Link Selection Policy | Auto |
| Frame Distribution Hash | Source/Destination IP address |

Once created the trunk shows up as an **interface**



Network » VLANs : VLAN List » New VLAN...

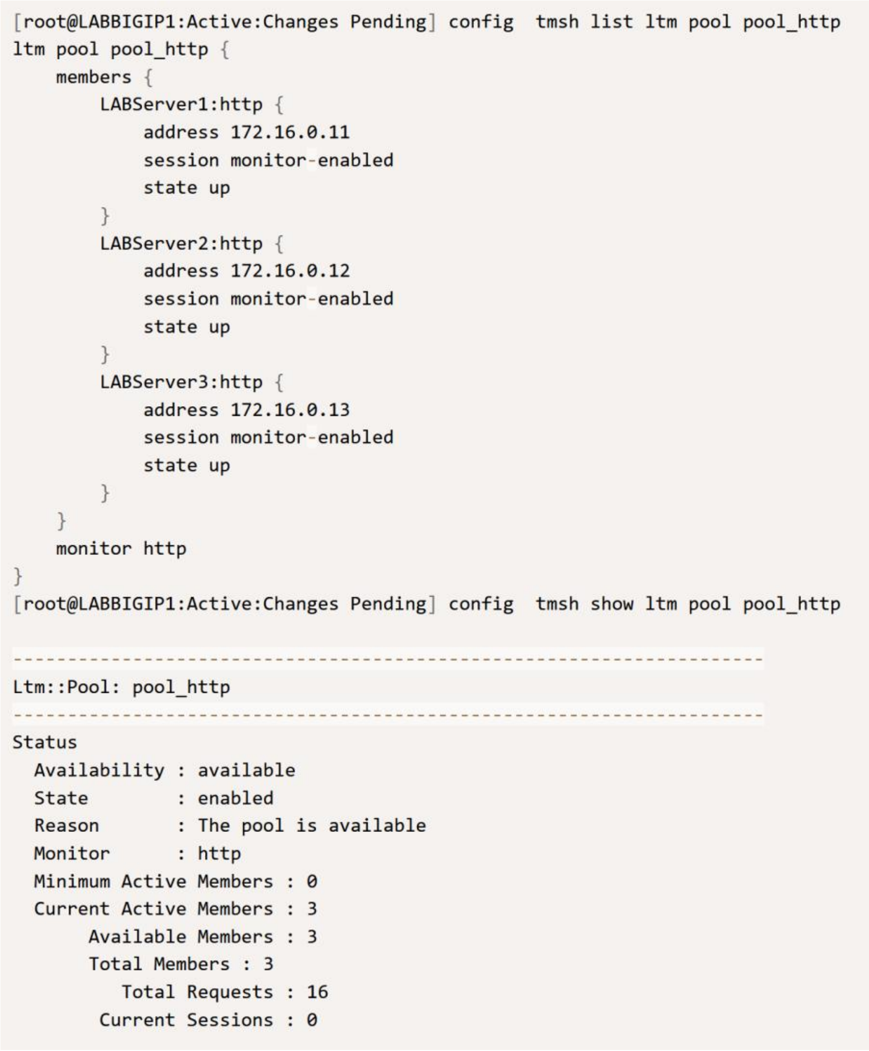
General Properties

| | |
|---|---|
| Name | |
| Description | |
| Tag | |

Resources

| | |
|---|---|
| Interfaces | Interface: 1.1 <br> Tagging: <br> Add <br> 1.1 <br> 1.2 <br> 1.3 <br> bigip-trunk* <br> Edit Delete |

# Command Line TMSH Introduction



```
[root@LABBIGIP1:Active:Changes Pending] config  tmsh list ltm pool pool_http
ltm pool pool_http {
    members {
        LABServer1:http {
            address 172.16.0.11
            session monitor-enabled
            state up
        }
        LABServer2:http {
            address 172.16.0.12
            session monitor-enabled
            state up
        }
        LABServer3:http {
            address 172.16.0.13
            session monitor-enabled
            state up
        }
    }
    monitor http
}
[root@LABBIGIP1:Active:Changes Pending] config  tmsh show ltm pool pool_http

---------------------------------------------------------------------
Ltm::Pool: pool_http
---------------------------------------------------------------------
Status
  Availability : available
  State        : enabled
  Reason       : The pool is available
  Monitor      : http
  Minimum Active Members : 0
  Current Active Members : 3
       Available Members : 3
       Total Members : 3
          Total Requests : 16
        Current Sessions : 0
```

**The structure of tmsh is hierarchical and modular.**

The highest level is the root module, which contains subordinate modules: **auth**, **cli**, gtm**, ltm**, **net**, **sys** and **wom**. Use the command help with no arguments to display the module hierarchy relative to the current module.

The **gtm (dns), ltm, net, sys,** and **wom** modules also contain subordinate modules. All modules and subordinate modules contain components.

To display the list of modules and components that are available in the current module press **Tab** or **?** at the tmsh prompt.

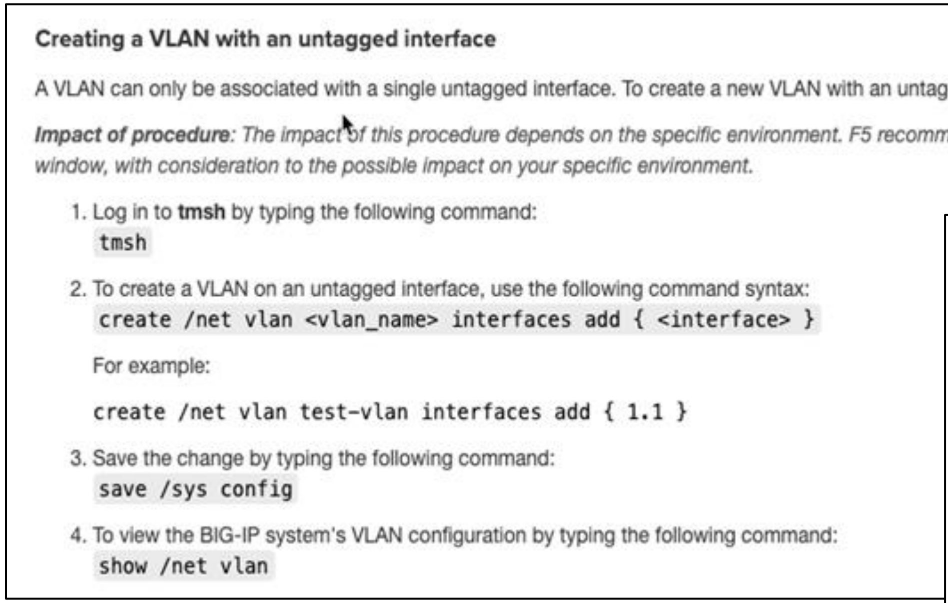
**tmsh list** – displays the configuration of an object(s)

**tmsh show** – displays the information of an object(s)

Examples of TMSH commands for VLAN, self-ip, and interfaces

https://support.f5.com/csp/article/K14961

# Creating untagged & tagged VLANs via TMSH commands

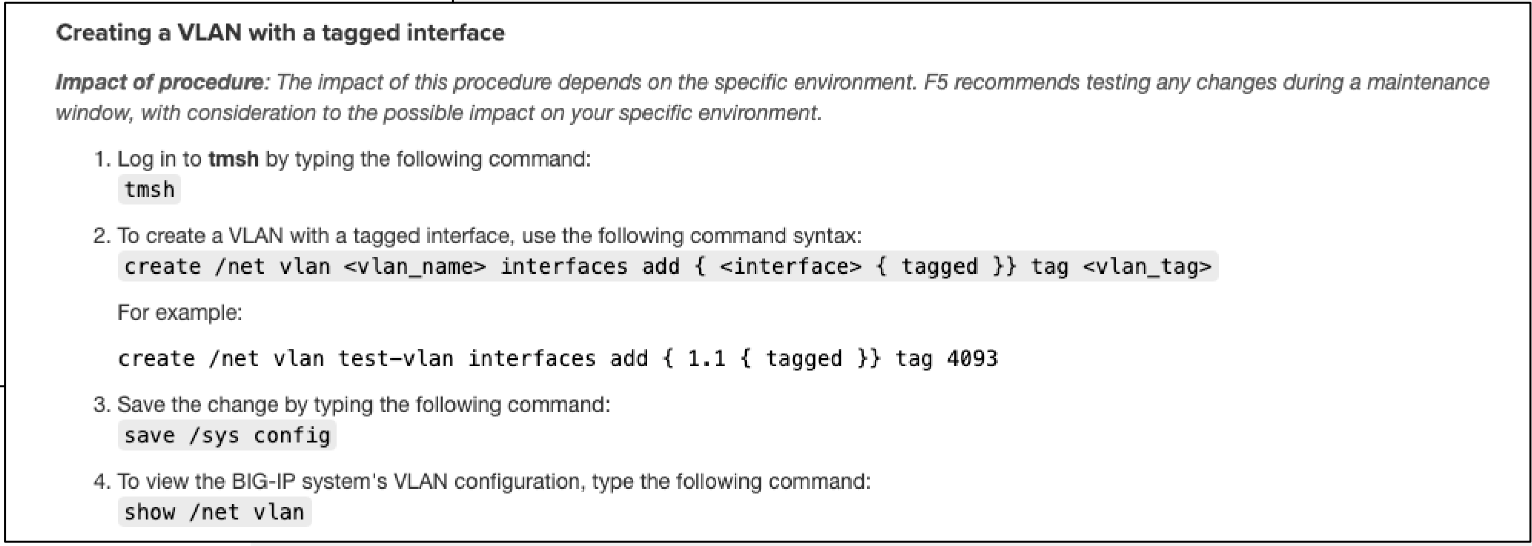


### Creating a VLAN with an untagged interface

A VLAN can only be associated with a single untagged interface. To create a new VLAN with an untagged interface, perform the following procedure:

***Impact of procedure**: The impact of this procedure depends on the specific environment. F5 recommends testing any changes during a maintenance window, with consideration to the possible impact on your specific environment.*

1. Log in to **tmsh** by typing the following command:
   ```
   tmsh
   ```
2. To create a VLAN on an untagged interface, use the following command syntax:
   ```
   create /net vlan <vlan_name> interfaces add { <interface> }
   ```
   For example:
   ```
   create /net vlan test-vlan interfaces add { 1.1 }
   ```
3. Save the change by typing the following command:
   ```
   save /sys config
   ```
4. To view the BIG-IP system's VLAN configuration by typing the following command:
   ```
   show /net vlan
   ```



### Creating a VLAN with a tagged interface

***Impact of procedure**: The impact of this procedure depends on the specific environment. F5 recommends testing any changes during a maintenance window, with consideration to the possible impact on your specific environment.*

1. Log in to **tmsh** by typing the following command:
   ```
   tmsh
   ```
2. To create a VLAN with a tagged interface, use the following command syntax:
   ```
   create /net vlan <vlan_name> interfaces add { <interface> { tagged }} tag <vlan_tag>
   ```
   For example:
   ```
   create /net vlan test-vlan interfaces add { 1.1 { tagged }} tag 4093
   ```
3. Save the change by typing the following command:
   ```
   save /sys config
   ```
4. To view the BIG-IP system's VLAN configuration, type the following command:
   ```
   show /net vlan
   ```

Examples of TMSH commands for VLANs, tagging and modifications

https://support.f5.com/csp/article/K14961

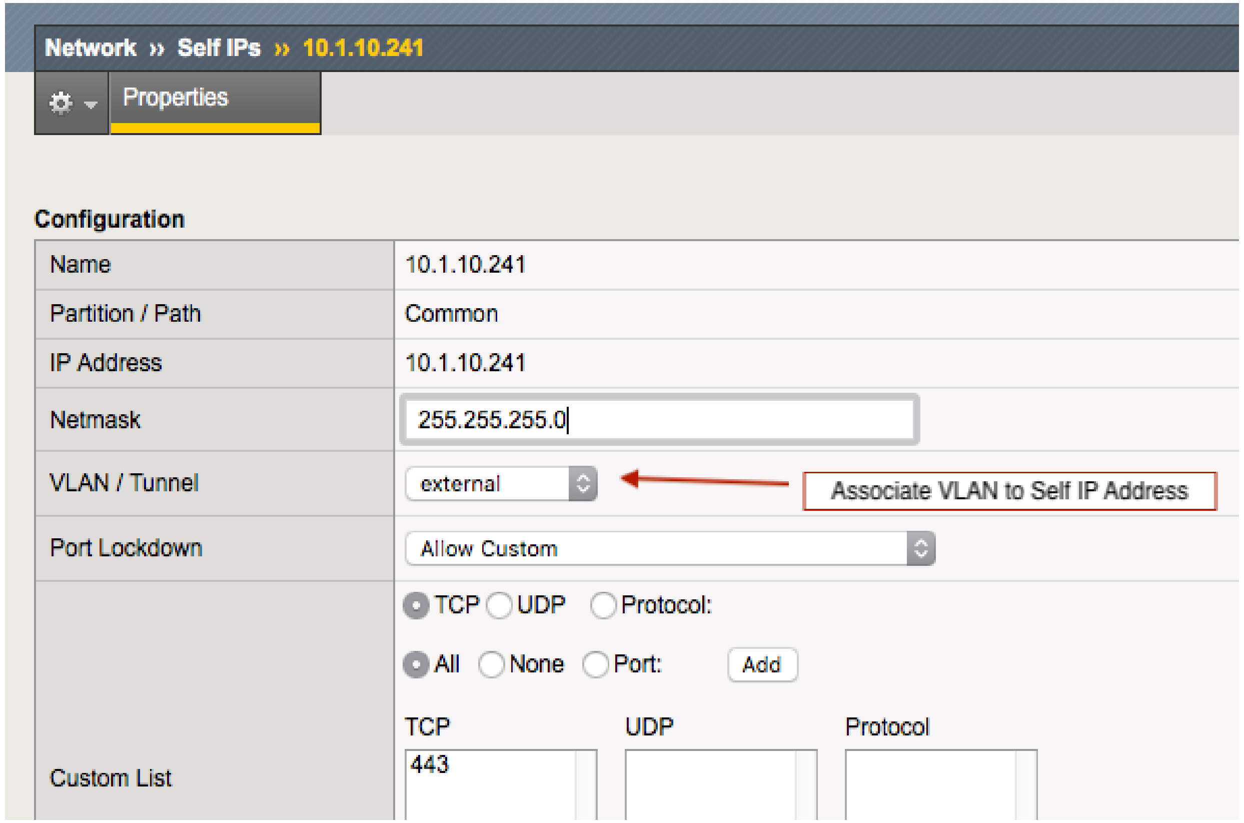
# Objective 1.01

Given a set of requirements, configure VLANs

## SELF IP

Determine appropriate layer 3 addressing for VLAN

- Layer 3 addressing for VLAN
- VLAN association with a self IP address



Network ›› Self IPs ›› 10.1.10.241

Configuration

| | |
|---|---|
| Name | 10.1.10.241 |
| Partition / Path | Common |
| IP Address | 10.1.10.241 |
| Netmask | 255.255.255.0 |
| VLAN / Tunnel | external |
| Port Lockdown | Allow Custom |
| | ● TCP ○ UDP ○ Protocol:<br>● All ○ None ○ Port: Add |
| Custom List | TCP: 443<br>UDP:<br>Protocol: |

Associate VLAN to Self IP Address

# Types of Self IPs

You should understand the difference between floating and non-floating self IPs. There are two types of self IP addresses that you can create:

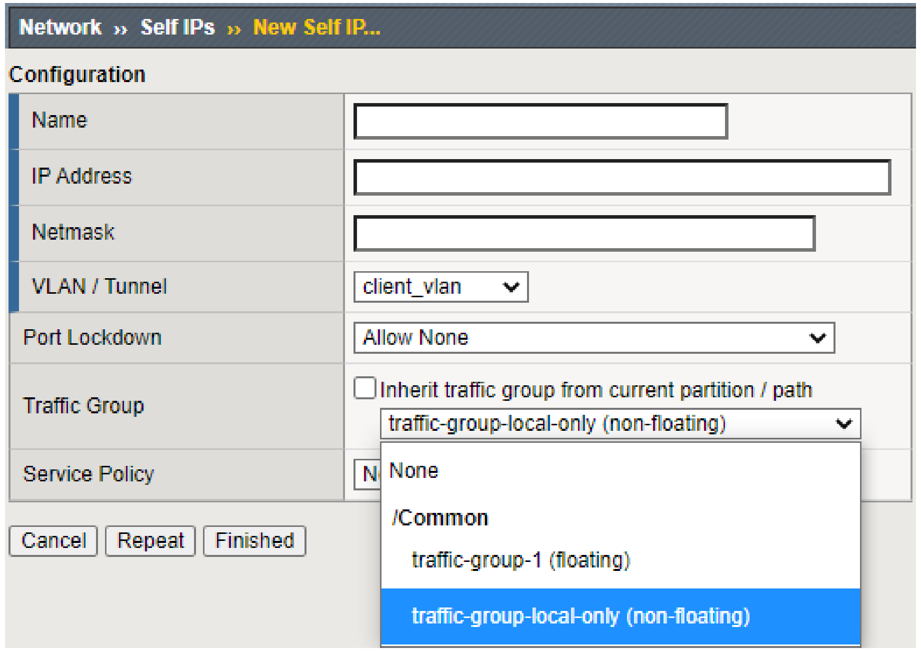
A **static (non-floating) self IP** address is an IP address that the BIG-IP system does not share with another BIG-IP system.

- Any self IP address that you assign to the default traffic group traffic-group-local-only is a static self IP address.
- If the BIG-IP goes down, the static self IPs go down with it.

A **floating self IP** address is an IP address that two BIG-IP systems share.

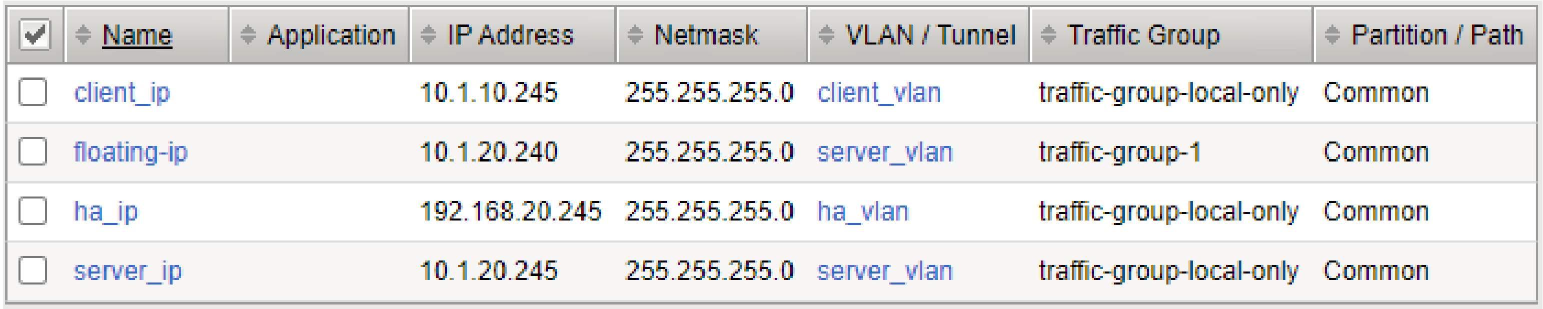
- Any self IP address that you assign to the default traffic group traffic-group-1 is a floating self IP address.
- Or any other traffic group that is NOT traffic-group-local-only
- A floating self IP only responds on the Active BIG-IP, if the Active BIG-IP goes down the floating self IP is activated on another BIG-IP in the Device Service Cluster

# Self IPs


Network » Self IPs » New Self IP...
Cancel
Repeat
Finished
None
/Common
traffic-group-1 (floating)
traffic-group-local-only (non-floating)

Configuration

| | |
|---|---|
| Name | |
| IP Address | |
| Netmask | |
| VLAN / Tunnel | client_vlan |
| Port Lockdown | Allow None |
| Traffic Group | □ Inherit traffic group from current partition / path<br>traffic-group-local-only (non-floating) |
| Service Policy | N |



| ☑ | Name | Application | IP Address | Netmask | VLAN / Tunnel | Traffic Group | Partition / Path |
|---|---|---|---|---|---|---|---|
| □ | client_ip | | 10.1.10.245 | 255.255.255.0 | client_vlan | traffic-group-local-only | Common |
| □ | floating-ip | | 10.1.20.240 | 255.255.255.0 | server_vlan | traffic-group-1 | Common |
| □ | ha_ip | | 192.168.20.245 | 255.255.255.0 | ha_vlan | traffic-group-local-only | Common |
| □ | server_ip | | 10.1.20.245 | 255.255.255.0 | server_vlan | traffic-group-local-only | Common |

```
(tmos)# list net self
net self floating-ip {
    address 10.1.20.240/24
    floating enabled
    traffic-group traffic-group-1
    unit 1
    vlan server_vlan
}
net self ha_ip {
    address 192.168.20.245/24
    allow-service {
        default
    }
    traffic-group traffic-group-local-only
    vlan ha_vlan
}
net self server_ip {
    address 10.1.20.245/24
    traffic-group traffic-group-local-only
    vlan server_vlan
}
net self client_ip {
    address 10.1.10.245/24
    traffic-group traffic-group-local-only
    vlan client_vlan
}
```

https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0/self-ip-addresses.html

# Creating Self IP via TMSH

## Create Self IP

```
tmsh create net self nameofip address IP address/netmask vlan vlan_name
```

```
tmsh create net self customer_vlan_ip address 10.1.20.241/24 vlan internal
```

Adds the self IP address **10.10.10.24** with name “customer_vlan_ip” to the VLAN named **internal**

## Modify Self IP

```
tmsh modify net self ipaddress/mask vlan vlan_name traffic-group traffic-group-name
```

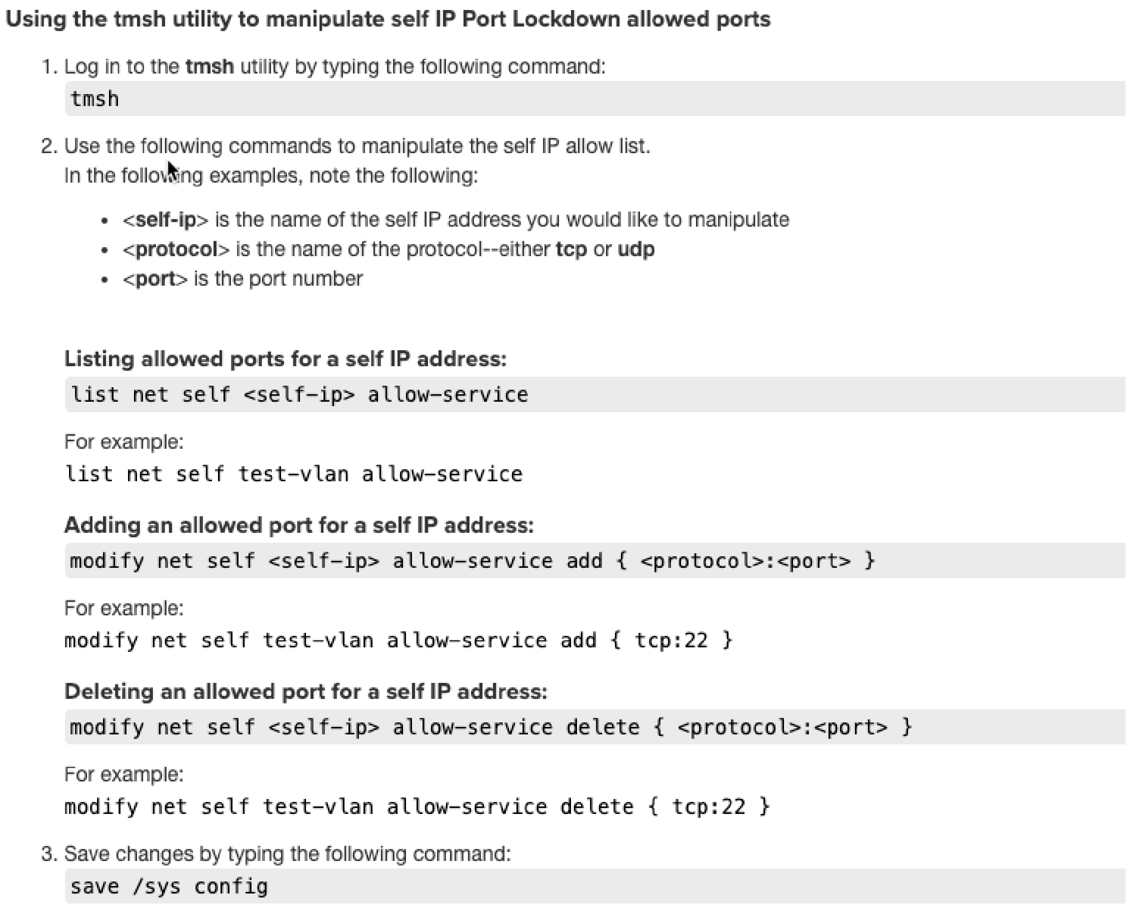
```
tmsh modify net self 10.1.1.1/16 vlan external traffic-group /common/traffic-group-1
       assigning ipaddress 10.1.1.1 to traffic group 1 (making it a floating ip)
```

**K14961: Create and modify VLANs using the tmsh utility**

https://my.f5.com/manage/s/article/K14961

# Port Lock down via TMSH or GUI

The port lockdown feature allows you to secure the BIG-IP system from unwanted connection attempts by controlling the level of access to each self IP address defined on the system.



**Using the tmsh utility to manipulate self IP Port Lockdown allowed ports**

1. Log in to the **tmsh** utility by typing the following command:

```
tmsh
```

2. Use the following commands to manipulate the self IP allow list.
   In the following examples, note the following:
   - <**self-ip**> is the name of the self IP address you would like to manipulate
   - <**protocol**> is the name of the protocol--either **tcp** or **udp**
   - <**port**> is the port number

   **Listing allowed ports for a self IP address:**

   ```
   list net self <self-ip> allow-service
   ```

   For example:

   ```
   list net self test-vlan allow-service
   ```

   **Adding an allowed port for a self IP address:**

   ```
   modify net self <self-ip> allow-service add { <protocol>:<port> }
   ```

   For example:

   ```
   modify net self test-vlan allow-service add { tcp:22 }
   ```

   **Deleting an allowed port for a self IP address:**

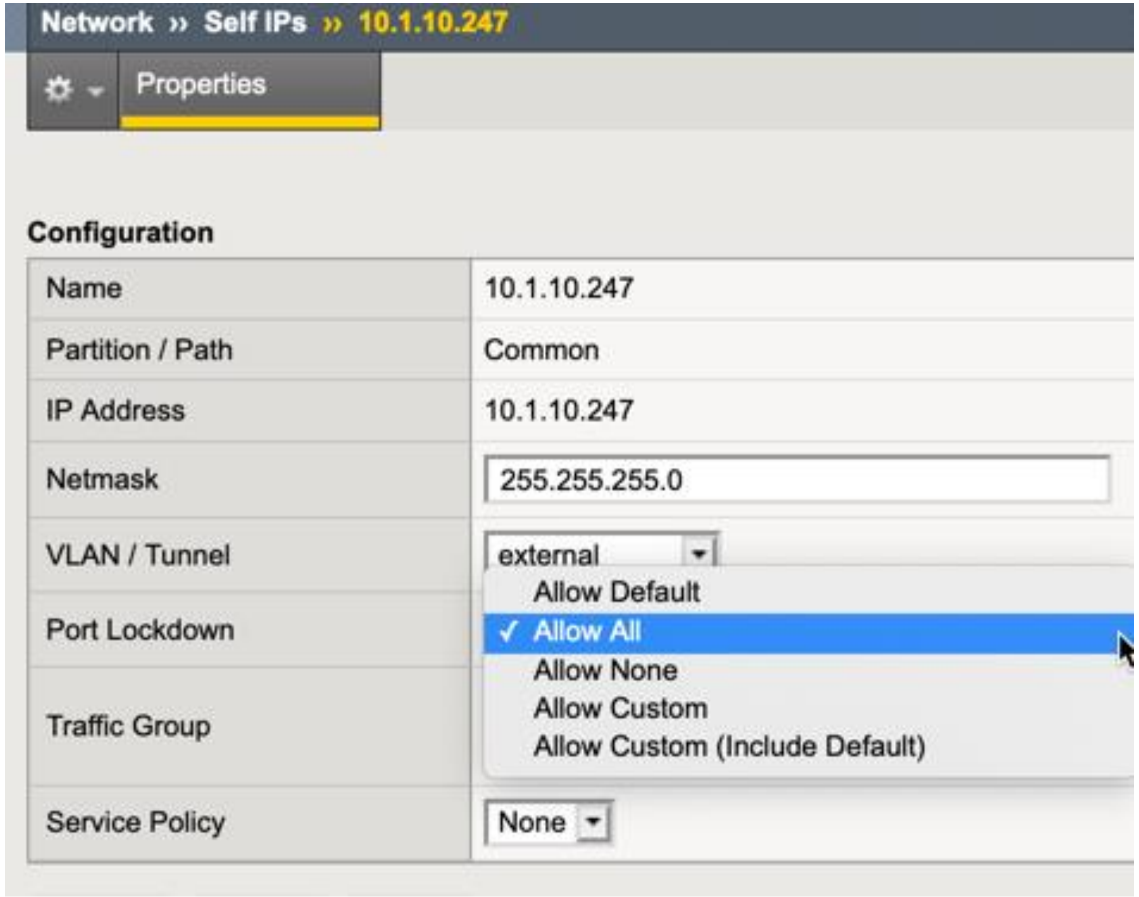
   ```
   modify net self <self-ip> allow-service delete { <protocol>:<port> }
   ```

   For example:

   ```
   modify net self test-vlan allow-service delete { tcp:22 }
   ```

3. Save changes by typing the following command:

```
save /sys config
```



Network » Self IPs » 10.1.10.247
Properties
Allow Default
✓ Allow All
Allow None
Allow Custom
Allow Custom (Include Default)

**Configuration**

| | |
|---|---|
| Name | 10.1.10.247 |
| Partition / Path | Common |
| IP Address | 10.1.10.247 |
| Netmask | 255.255.255.0 |
| VLAN / Tunnel | external |
| Port Lockdown | ✓ Allow All |
| Traffic Group | |
| Service Policy | None |

**K17333: Overview of port lockdown behavior (12.x - 17.x)**
https://my.f5.com/manage/s/article/K17333

# Objective 1.02

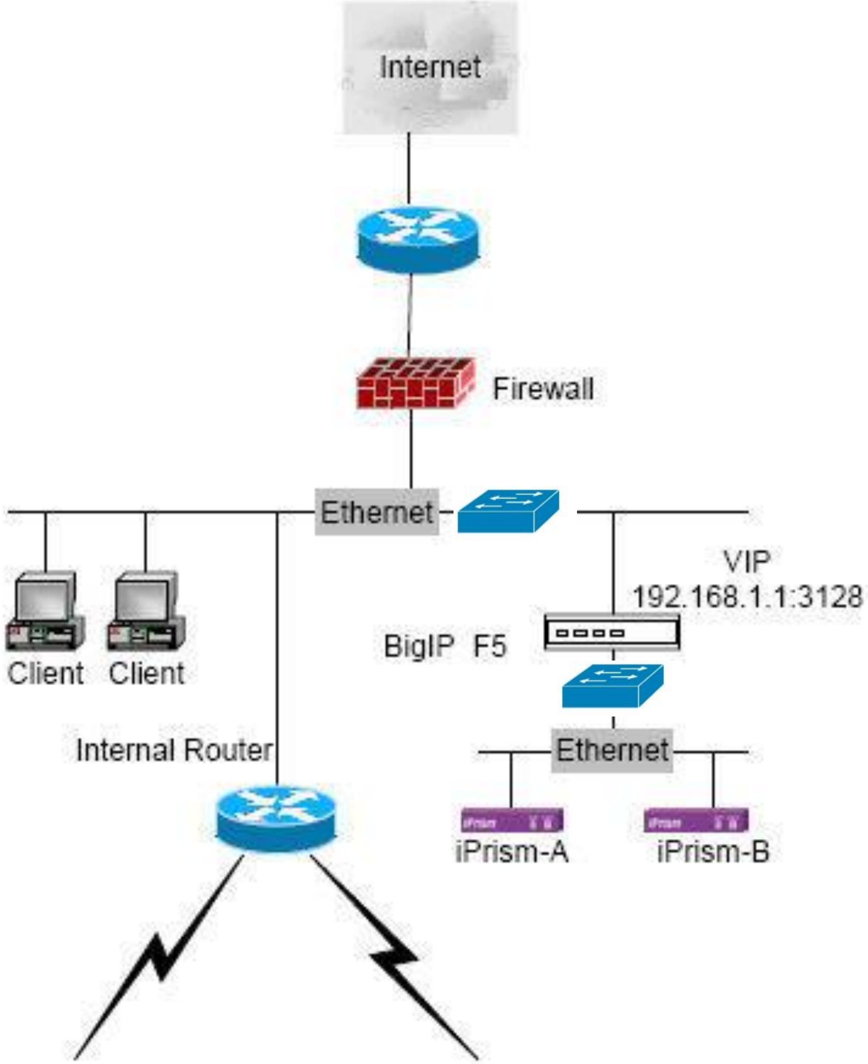
Determine switch, router, & application connectivity requirements

Explain the function and purpose of a router, of a firewall and of a switch.

**Router:** Layer 3 – receives and forwards data packets between computer networks (WAN).

**Firewall:** Layer 3, 4 – monitors & controls incoming/outgoing network traffic

**Switch:** Layer 2 – connects devices using packet switching (LAN)

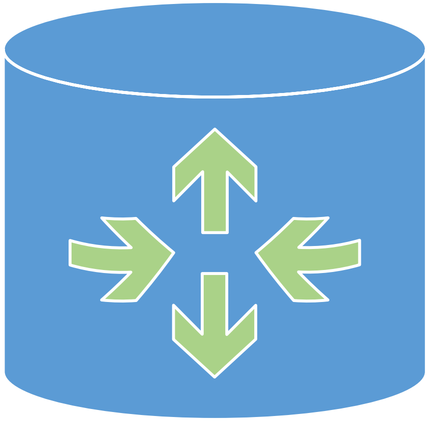


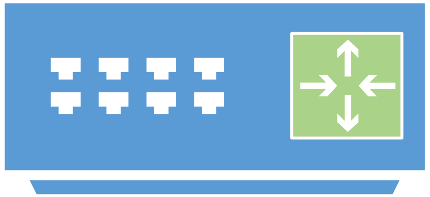
# Objective 1.02

## Determine switch, router, & application connectivity requirements

**Routers: Layer 3**

- Routers (directs) network traffic based on IP address and Protocol
- A routing protocol specifies the criteria and rules to use to send the data packets. It could be hop based, time based etc.
- Routers maintain routing tables – constantly updating them depending on comms with other routers
- Routers usually connect LANs/CANs to WANs
- Routers can prioritize data
- Some types are Core, Edge, Wireless, Virtual





# Objective 1.02

Determine switch, router, & application connectivity requirements

**Firewall: Traditionally Layer 3 & 4 -  Now up to layer 7**

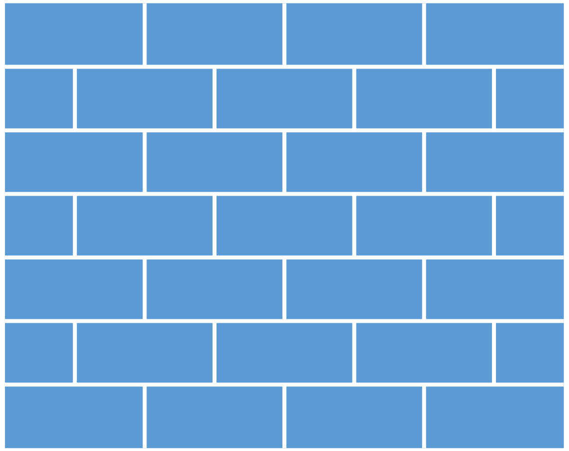
Works as a gate guard for networks and applications – creates a barrier between protected and unprotected networks.

**Traditional:** IP address checks and ports and protocol (tcp or udp)

- Data coming or destined to certain IP addresses or Ports allowed/blocked based on policy

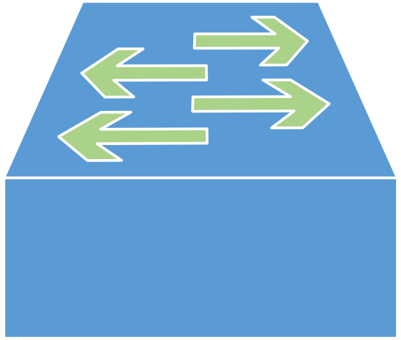
**Modern:** Traffic type and/or content

- Inspect content for bad traffic (executables, scripts, SQL injection, etc.)
- Web Application Firewall (WAF), Web Application API Protection (WAAP, securing API endpoints)



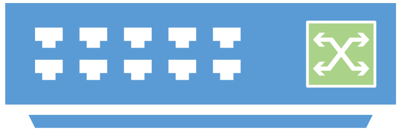
# Objective 1.02

## Determine switch, router, & application connectivity requirements



**Switches: Layer 2 & 3**

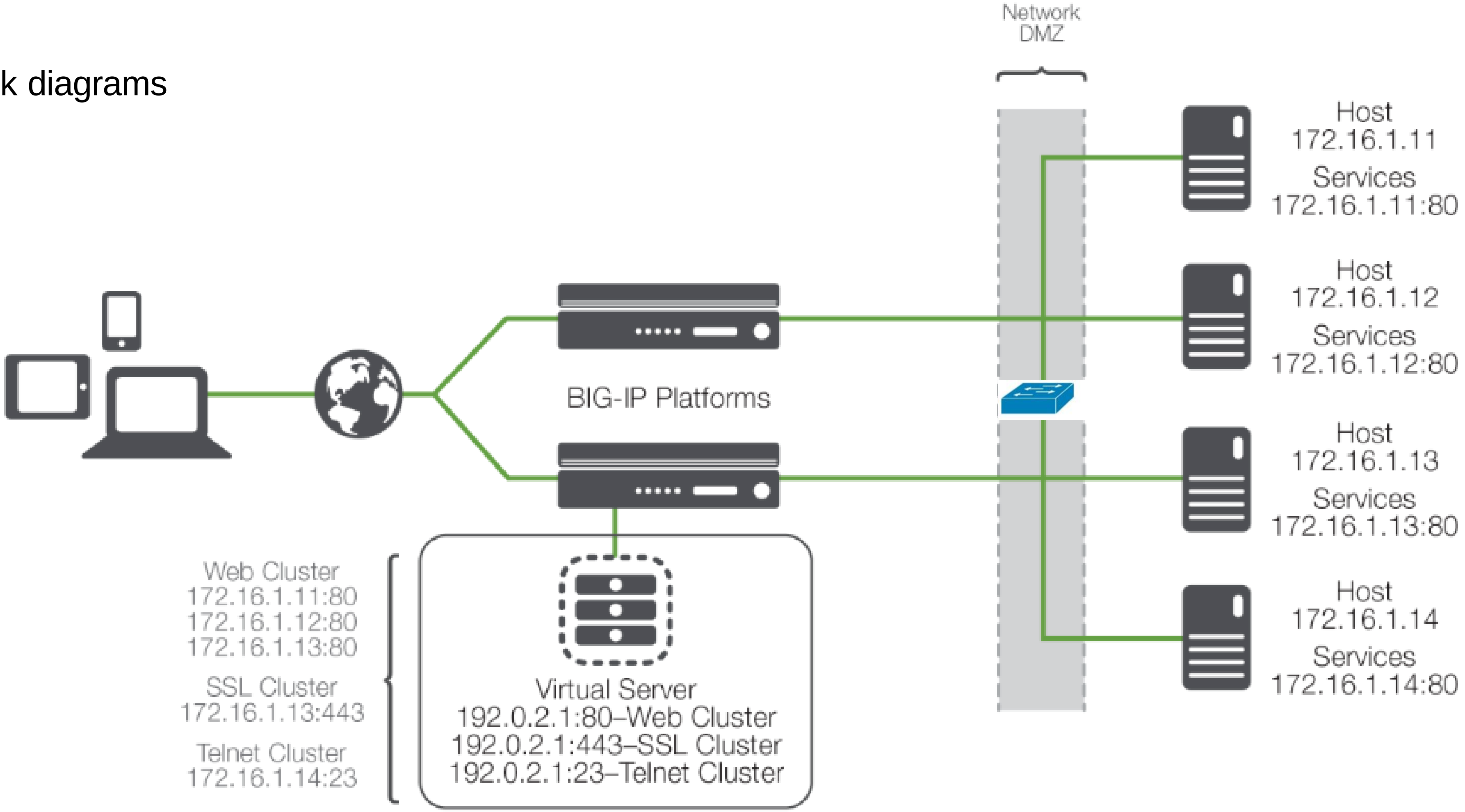
- Connects networked devices within a LAN/CAN using packet switching
- Uses Media Access Control (MAC) addresses to forward data at layer 2 - smart switches can also work at layer 3 – Multilayer or Smart Switches
- Network packets get turned into ”Frames” with Source/Destination MAC
- Switches create a collision domain per port vs hubs that are all part of collision domain



# Objective 1.02

Determine switch, router, & application connectivity requirements

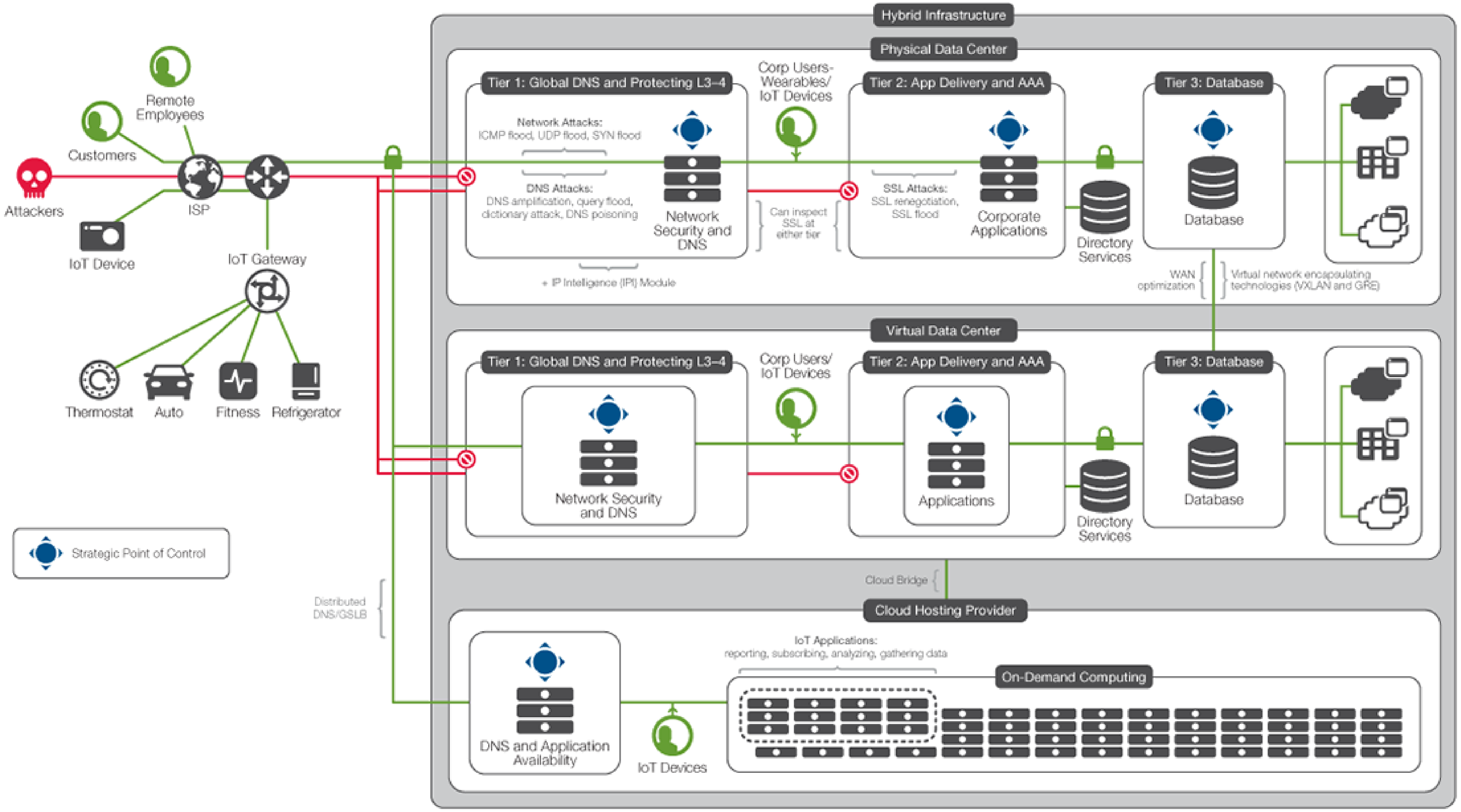
Interpret network diagrams



# Objective 1.02

Determine switch, router, & application connectivity requirements

Interpret network diagrams


Hybrid Infrastructure
Physical Data Center
Remote Employees
Customers
Attackers
ISP
IoT Device
IoT Gateway
Thermostat
Auto
Fitness
Refrigerator
Tier 1: Global DNS and Protecting L3–4
Network Attacks:
ICMP flood, UDP flood, SYN flood
DNS Attacks:
DNS amplification, query flood, dictionary attack, DNS poisoning
Network Security and DNS
+ IP Intelligence (IPI) Module
Corp Users-Wearables/ IoT Devices
Can inspect SSL at either tier
Tier 2: App Delivery and AAA
SSL Attacks:
SSL renegotiation, SSL flood
Corporate Applications
Directory Services
Tier 3: Database
Database
WAN optimization
Virtual network encapsulating technologies (VXLAN and GRE)
Virtual Data Center
Tier 1: Global DNS and Protecting L3–4
Network Security and DNS
Corp Users/ IoT Devices
Tier 2: App Delivery and AAA
Applications
Directory Services
Tier 3: Database
Database
Strategic Point of Control
Distributed DNS/GSLB
Cloud Bridge
Cloud Hosting Provider
DNS and Application Availability
IoT Devices
IoT Applications:
reporting, subscribing, analyzing, gathering data
On-Demand Computing

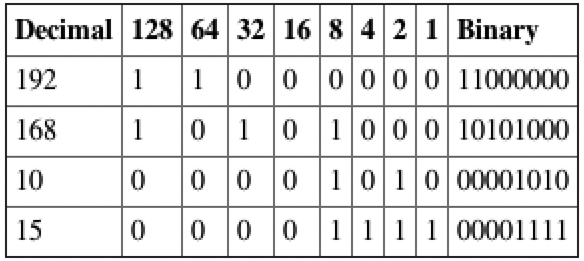
# Objective 1.03

Given a set of requirements, assign IP addresses

## IP addresses and Subnetting

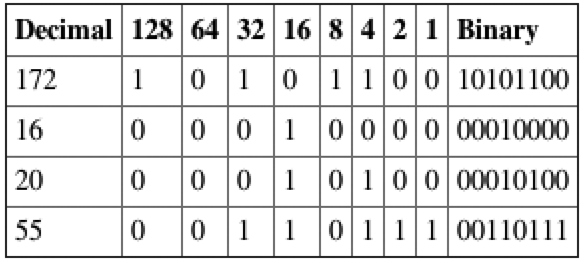
- **IP:** 32 bits, 4 octets, 0-255 (256 values)
- **Netmask:** Defines how many bits are for network and how many for the host addresses
- Within each octet position values are: **128 64 32 16 8 4 2 1** → added up equals **255** per octet
- 192.168.4.40/25 → **/25** means take **25 bits** for the network (**netmask**) → 255.255.255.128
- 192.168.4.40 → convert IP to binary → 11000000.10101000.00000100.00101000
- Apply netmask in binary → 11111111 . 11111111 . 11111111. 10000000
  - Hosts = 2 to the x power (how many 0s)
  - Networks: 2 to the x power (how many 1s in octet)

### IP Address: 192.168.10.15



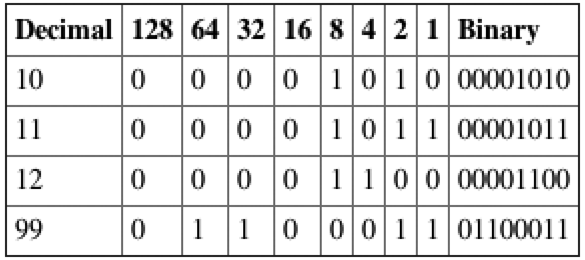
| Decimal | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Binary |
|---|---|---|---|---|---|---|---|---|---|
| 192 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 11000000 |
| 168 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 10101000 |
| 10 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 00001010 |
| 15 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 00001111 |

### IP Address: 172.16.20.55



| Decimal | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Binary |
|---|---|---|---|---|---|---|---|---|---|
| 172 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 10101100 |
| 16 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 00010000 |
| 20 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 00010100 |
| 55 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 00110111 |

### IP Address: 10.11.12.99



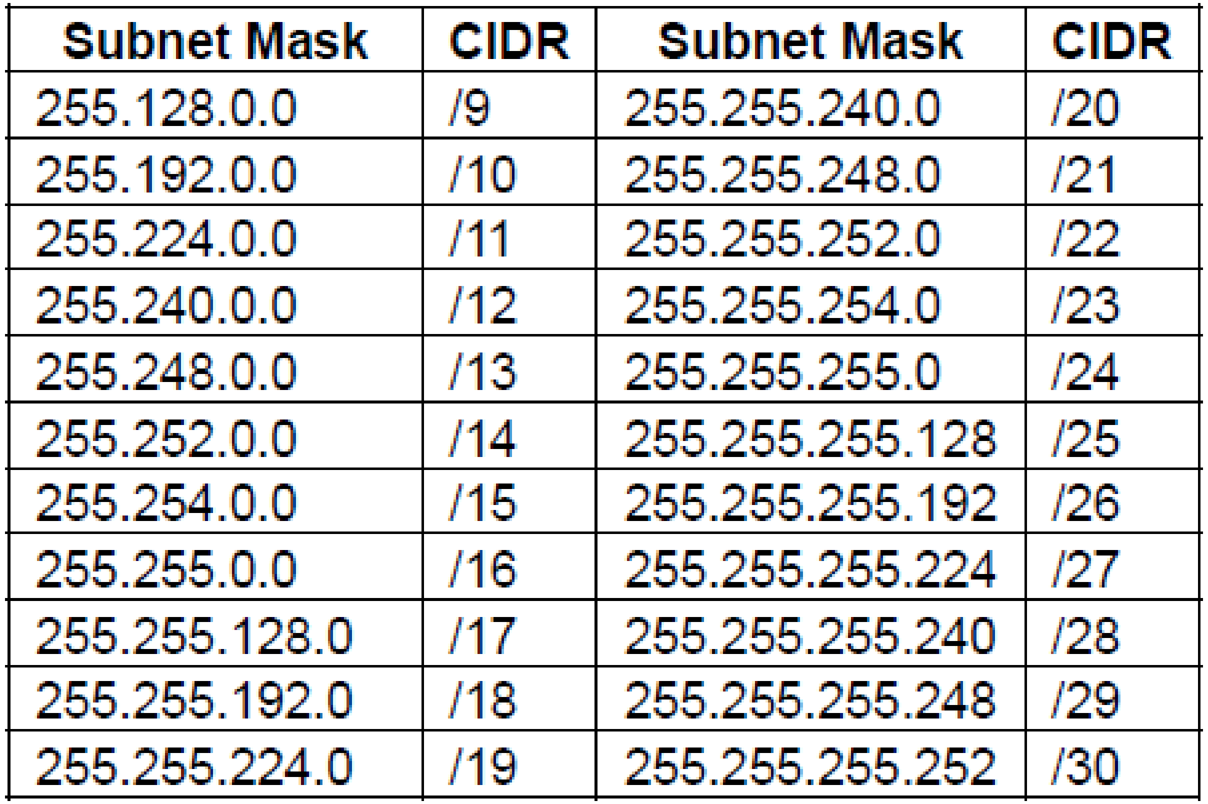
| Decimal | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Binary |
|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 00001010 |
| 11 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 00001011 |
| 12 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 00001100 |
| 99 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 01100011 |

# Objective 1.03

Given a set of requirements, assign IP addresses

**Interpret address and subnet relationships**

- Given notation of 195.14.6.2/25, what is the network address, last useable address and netmask?
  - 195.14.6.0, 195.14.6.126, 255.255.255.128
- Given notations of 201.10.11.22/28, what addresses are in my network and what is the network address?
  - 201.10.11.22 → convert IP to binary → 11001001.00001010.00001011.00010110
  - Apply netmask in binary → 11111111 . 11111111 . 11111111. 11110000
  - Hosts = 2 to the power of 4 (how many 0s) Networks: 2 to the power of 4 (how man 1s in octet)
  - 255.255.255.240 netmask, 16 networks 16 host, 201.10.11.16-32, 17-30 useable



| Subnet Mask | CIDR | Subnet Mask | CIDR |
|---|---|---|---|
| 255.128.0.0 | /9 | 255.255.240.0 | /20 |
| 255.192.0.0 | /10 | 255.255.248.0 | /21 |
| 255.224.0.0 | /11 | 255.255.252.0 | /22 |
| 255.240.0.0 | /12 | 255.255.254.0 | /23 |
| 255.248.0.0 | /13 | 255.255.255.0 | /24 |
| 255.252.0.0 | /14 | 255.255.255.128 | /25 |
| 255.254.0.0 | /15 | 255.255.255.192 | /26 |
| 255.255.0.0 | /16 | 255.255.255.224 | /27 |
| 255.255.128.0 | /17 | 255.255.255.240 | /28 |
| 255.255.192.0 | /18 | 255.255.255.248 | /29 |
| 255.255.224.0 | /19 | 255.255.255.252 | /30 |

# Objective 1.03

Given a set of requirements, assign IP addresses

Understand public/private, multicast addressing, and broadcast concepts

**5 Classes of IPv4 addresses:** A,B,C,D,E – only talk about A,B,C

- A: 1.0.0.0 – 127.0.0.0 /8
- B: 128.0.0.0 – 191.255.0.0 /16
- C: 192.0.0.0 – 223.255.255.0 /24

**IPv4 Private Addresses**

- A: 10.0.0.0 /8
- B:172.16.0.0 /12 (172.16. – 172.31.)
- C:192.168.0.0 /16

RFC1918 – IPv4 Public & Private Address Space

Multicast Addressing – 224.0.0.0 thru 239.255.255.255 – Video conferencing

Broadcast IP – All hosts, ex: 255.255.255.255

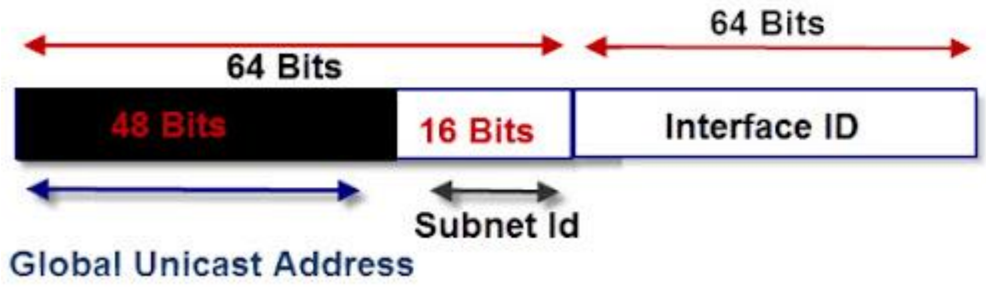
Classless Interdomain Routing (CIDR)/supernetting saves address space, more efficient

# Objective 1.03

Given a set of requirements, assign IP addresses

**A valid IPv6 address = 128 bits**

- 8 groups of 4 hexadecimal digits (0-9,a-f) separated by colons
  - **2345:0425:2CA1:0000:0000:0567:5673:23b5**
- Leading 0's can be omitted when writing it. The above can be written like:
  - **2345:425:2CA1:0:0:567:5673:23b5**
- Contiguous 0's can be omitted: The above can be written like:
  - **2345:425:2CA1::567:5673:23b5**
- Contiguous 0's can only be abbreviated once as ::, otherwise they must show :0:0
- Example: convert IPv4 127.0.0.1 to IPv6 (https://tools.ietf.org/html/rfc2373)
- http://www.ciscopress.com/articles/article.asp?p=2803866


64 Bits

64 Bits

48 Bits

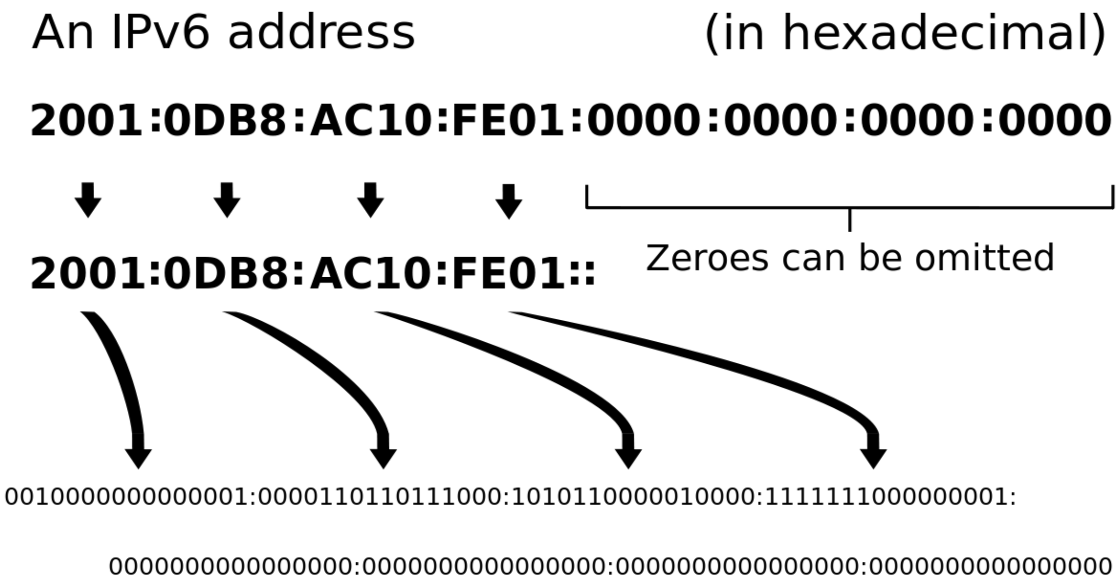
16 Bits

Interface ID

Subnet Id

Global Unicast Address

IPv6 Address Structure


An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01::

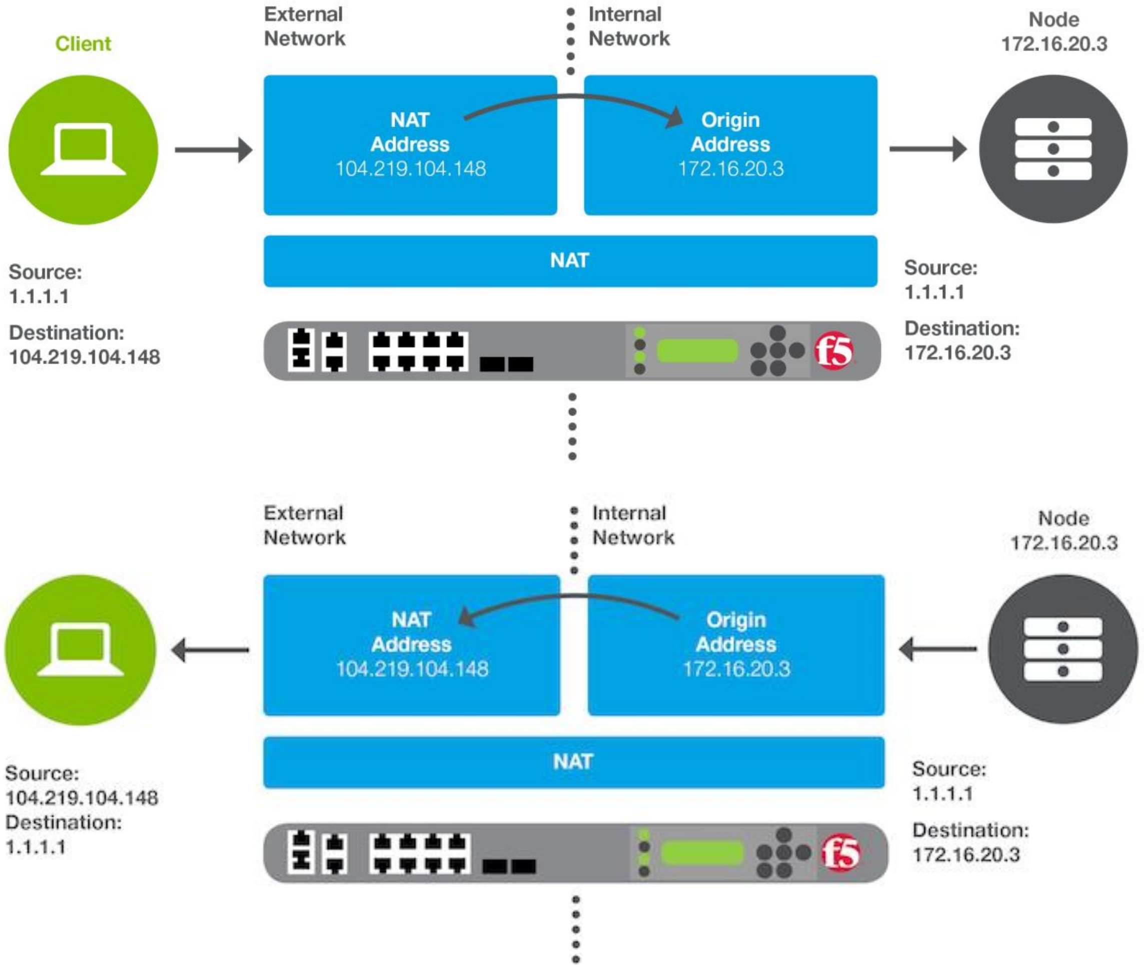
Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

# Objective 1.03

Given a set of requirements, assign IP addresses



## Explain the function and purpose of NAT

### Purpose of NAT

A **Network Address Translation (NAT)** is a mapping of one IP address to another IP address. This mapping can be a translation of source, destination, or both. A NAT can be outbound or inbound.

### Outbound NAT

Outbound NAT translates an internal source address to a public address. A NAT can also be used to translate an internal node's IP address to an Internet routable IP address.

### Inbound NAT

Inbound NAT translates a public destination address to an internal address. When an external client sends traffic to the public IP address defined in a NAT, BIG-IP translates that destination address to the internal node IP address.

# Objective 1.03

Given a set of requirements, assign IP addresses

### Explain the function and purpose of DHCP

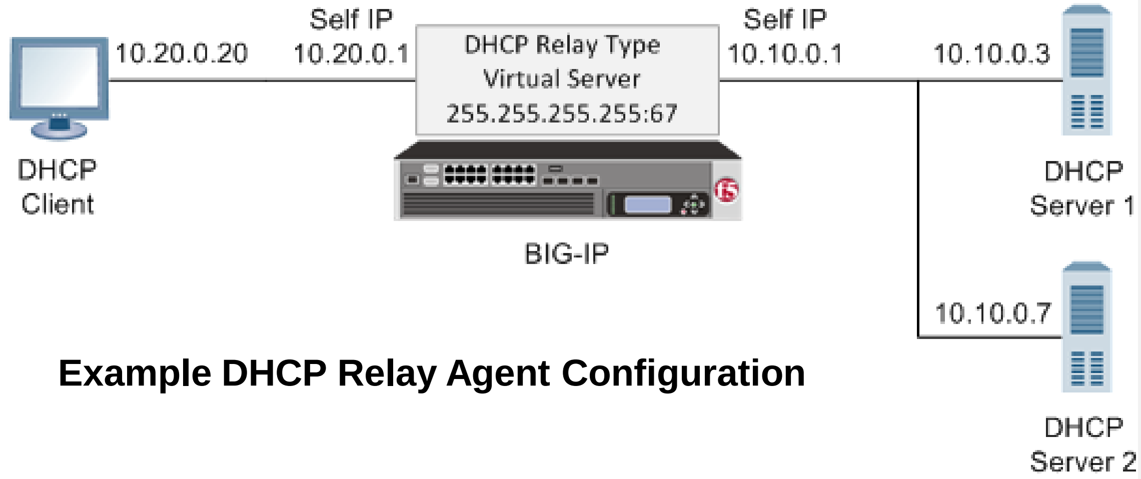
- Purpose of DHCP – network management protocol
- Managing IP addresses for DHCP clients
- About the BIG-IP system as a DHCP relay agent
- Server listens on 67, client on 68 UDP

### Configuring the BIG-IP System as a DHCP Relay Agent:

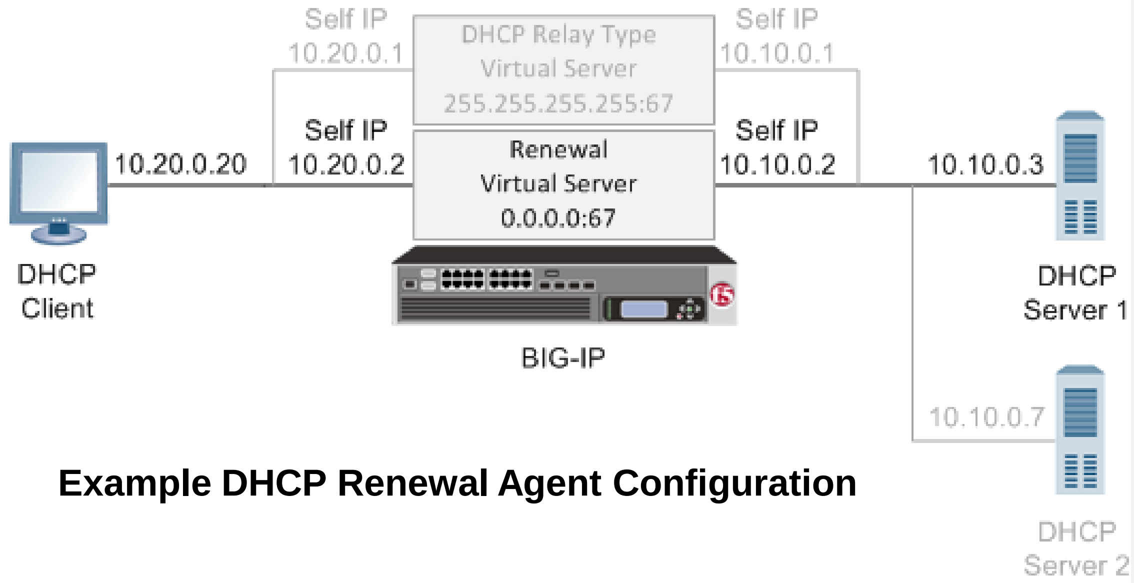
https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-local-traffic-manager-implementations/configuring-the-big-ip-system-as-a-dhcp-relay-agent.html

### Configuring the BIG-IP System for DHCP Renewal:

https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-local-traffic-manager-implementations/configuring-the-big-ip-system-for-dhcp-renewal.html



**Example DHCP Relay Agent Configuration**



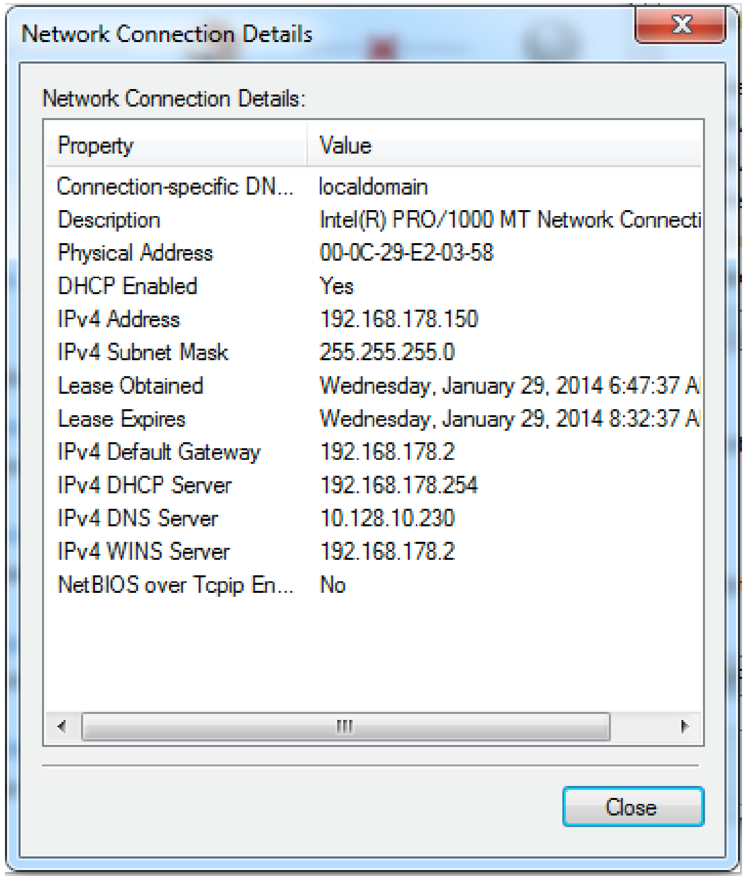
**Example DHCP Renewal Agent Configuration**

# Objective 1.04

Identify a valid MAC address

## MAC address

- Known as the hardware address while the IP address is the logical address of the device.
- 6 groups of 2 hexadecimal digits (0-9,a-f), 48 bits
- MAC addresses can appear in several formats



Network Connection Details:

| Property | Value |
|---|---|
| Connection-specific DN... | localdomain |
| Description | Intel(R) PRO/1000 MT Network Connecti |
| Physical Address | 00-0C-29-E2-03-58 |
| DHCP Enabled | Yes |
| IPv4 Address | 192.168.178.150 |
| IPv4 Subnet Mask | 255.255.255.0 |
| Lease Obtained | Wednesday, January 29, 2014 6:47:37 A |
| Lease Expires | Wednesday, January 29, 2014 8:32:37 A |
| IPv4 Default Gateway | 192.168.178.2 |
| IPv4 DHCP Server | 192.168.178.254 |
| IPv4 DNS Server | 10.128.10.230 |
| IPv4 WINS Server | 192.168.178.2 |
| NetBIOS over Tcpip En... | No |

28:cf:e9:1b:ae:91

28cf.e91b.ae91

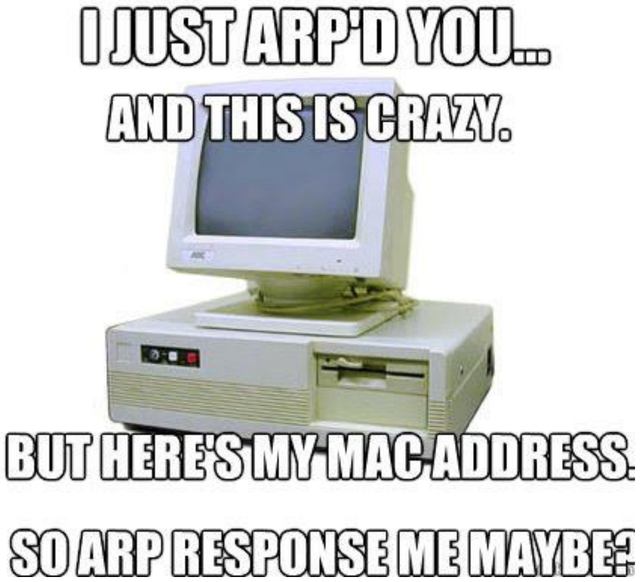
28-cf-e9-1b-ae-91

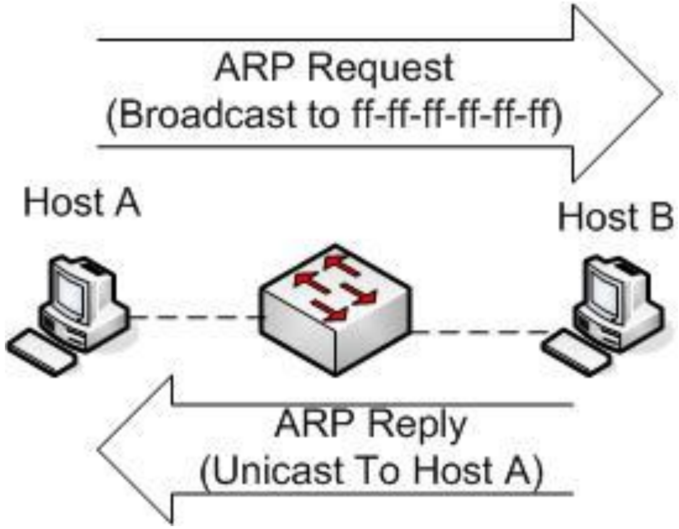
```
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST>
mtu 1500
          ether 28:cf:e9:1b:ae:91
          inet6 fe80::2acf:e9ff:fe1b:ae91%en0 prefixlen 64 scopeid 0x4
          inet 192.168.69.109 netmask 0xffffff00 broadcast
192.168.69.255
          nd6 options=1<PERFORMNUD>
          media: autoselect
          status: active
```

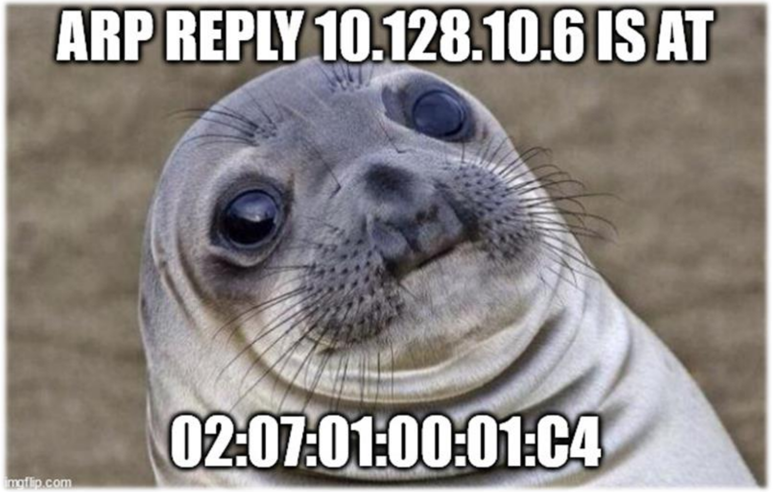
# Objective 1.04

Define ARP and explain what it does

Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.







**arp who-has 10.128.10.6 tell 10.128.10.68**
**arp reply 10.128.10.6 is-at 02:07:01:00:01:c4**

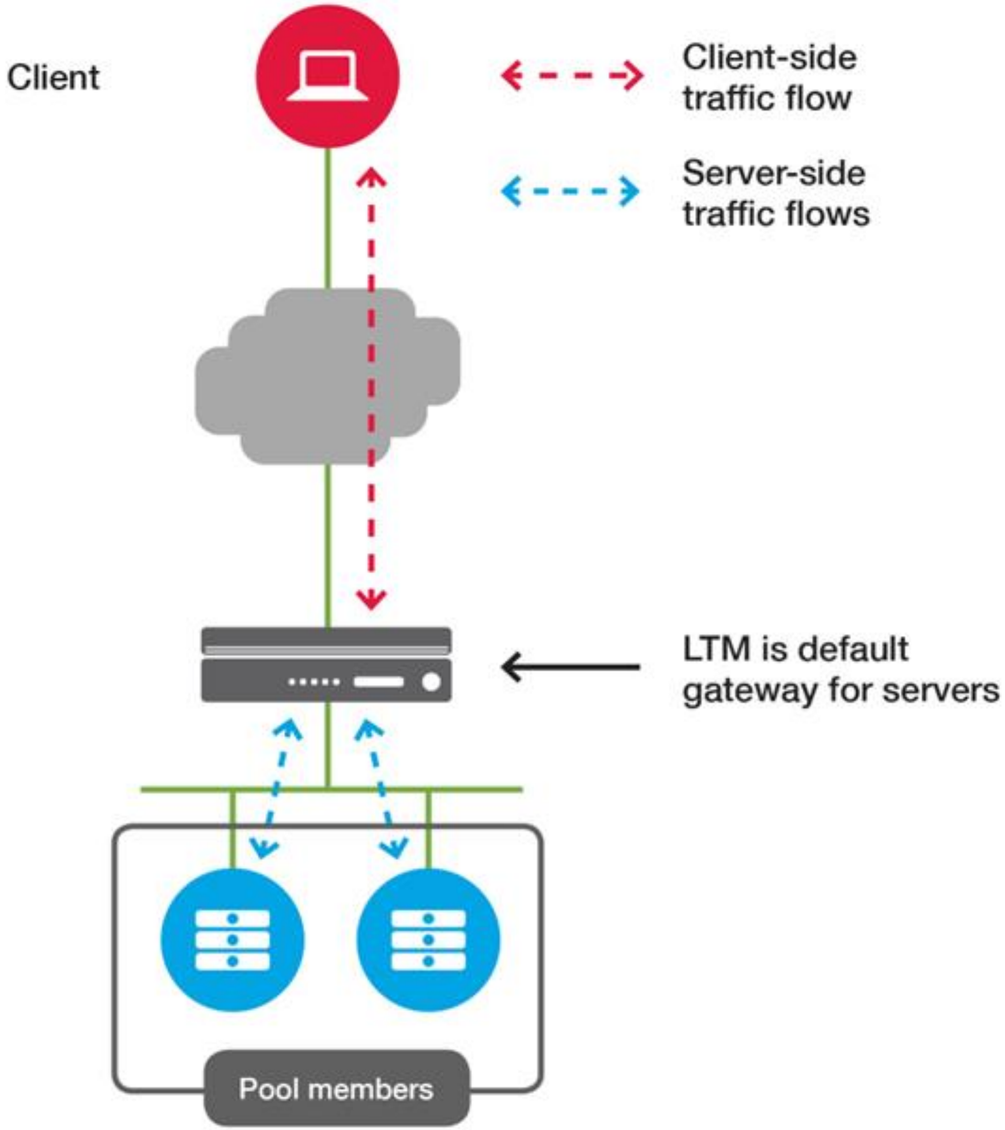
# Objective 1.04

State the purpose of a default gateway

**Default Gateway**

A default gateway is the node in a computer network using the internet protocol suite that serves as the forwarding host (router) to other networks, when no other route specification matches the destination IP address of a packet.

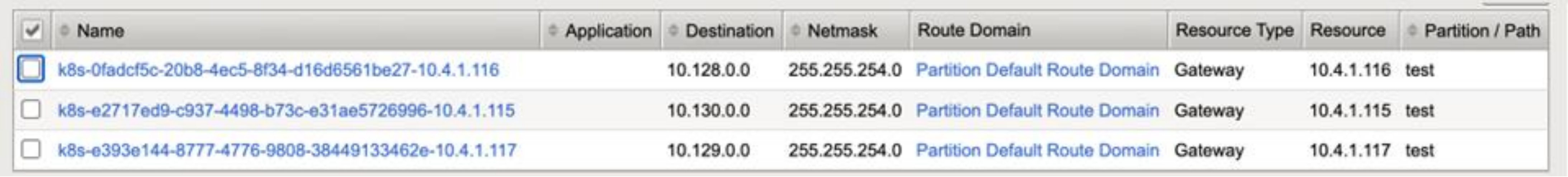
**The Default Gateway is also known as the Gateway of Last Resort**



# Objective 1.05

Explain why a route is needed

- Part of managing routing on a BIG-IP system is to add static routes for destinations that are not located on the directly-connected network.
- Routing is the process of selecting a path for traffic between networks or across multiple networks
- https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0/static-routes.html
- Dynamic routing protocols supported:
  - BGP4, IS-IS, OSPFv2, OSPFv3, PIM, RIPv1, RIPv2, RIPng, (BFD is static)



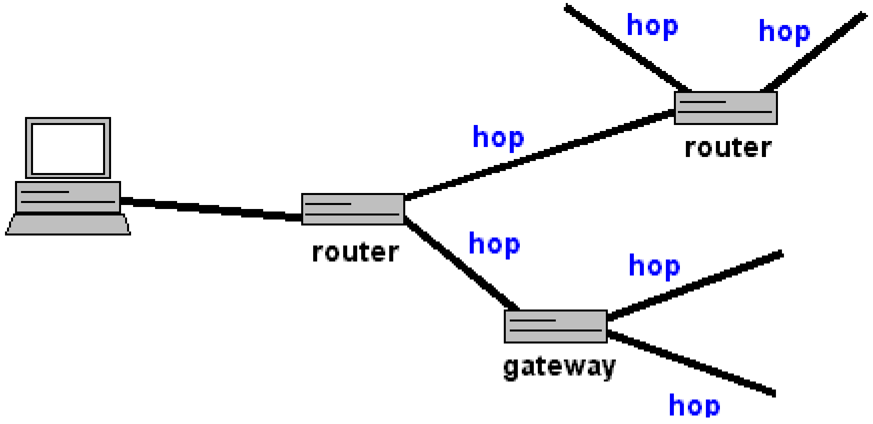
| ☑ | Name | Application | Destination | Netmask | Route Domain | Resource Type | Resource | Partition / Path |
|---|---|---|---|---|---|---|---|---|
| □ | k8s-0fadcf5c-20b8-4ec5-8f34-d16d6561be27-10.4.1.116 | | 10.128.0.0 | 255.255.254.0 | Partition Default Route Domain | Gateway | 10.4.1.116 | test |
| □ | k8s-e2717ed9-c937-4498-b73c-e31ae5726996-10.4.1.115 | | 10.130.0.0 | 255.255.254.0 | Partition Default Route Domain | Gateway | 10.4.1.115 | test |
| □ | k8s-e393e144-8777-4776-9808-38449133462e-10.4.1.117 | | 10.129.0.0 | 255.255.254.0 | Partition Default Route Domain | Gateway | 10.4.1.117 | test |

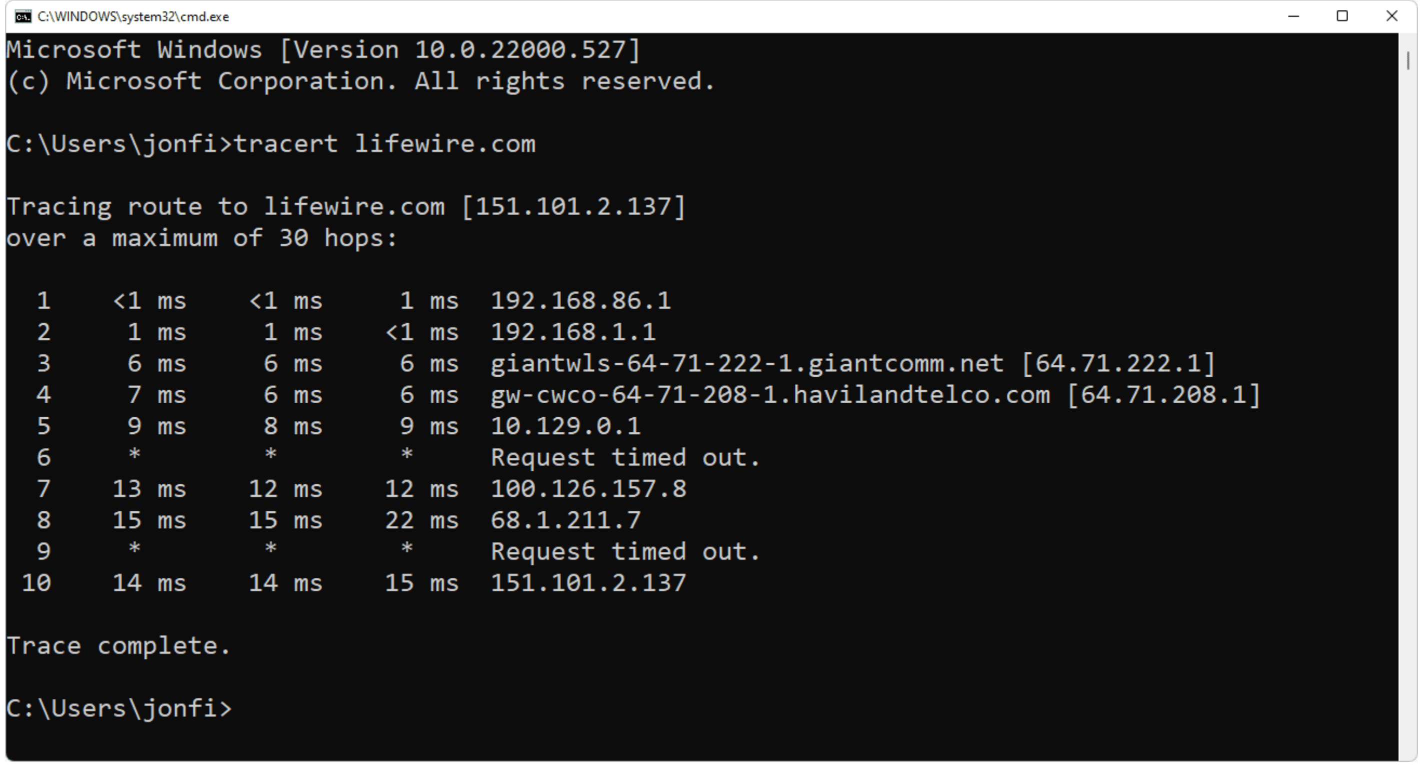
# Objective 1.05

## Explain network hops

Network hops refers to the number of networking devices between the sending unit and the final destination of the communication.

Some or all of these devices can make changes to the datagram in the flow and some dynamic routing protocols use hop count as a metric in determining the best path.



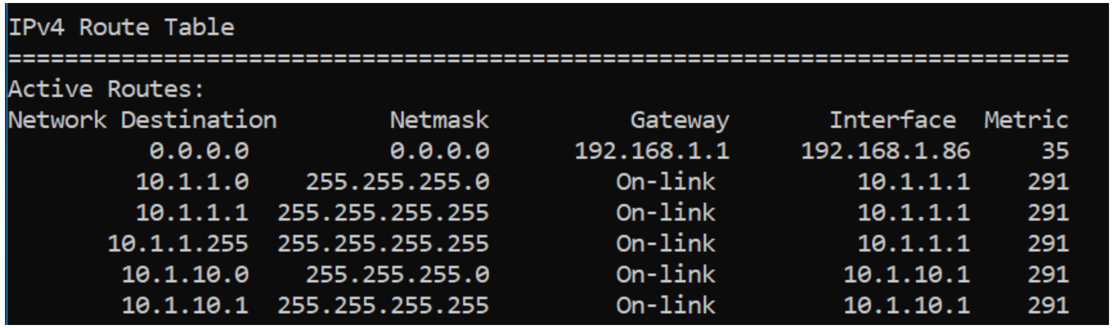


```
Microsoft Windows [Version 10.0.22000.527]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jonfi>tracert lifewire.com

Tracing route to lifewire.com [151.101.2.137]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  192.168.86.1
  2     1 ms     1 ms    <1 ms  192.168.1.1
  3     6 ms     6 ms     6 ms  giantwls-64-71-222-1.giantcomm.net [64.71.222.1]
  4     7 ms     6 ms     6 ms  gw-cwco-64-71-208-1.havilandtelco.com [64.71.208.1]
  5     9 ms     8 ms     9 ms  10.129.0.1
  6     *        *        *     Request timed out.
  7    13 ms    12 ms    12 ms  100.126.157.8
  8    15 ms    15 ms    22 ms  68.1.211.7
  9     *        *        *     Request timed out.
 10    14 ms    14 ms    15 ms  151.101.2.137

Trace complete.

C:\Users\jonfi>
```

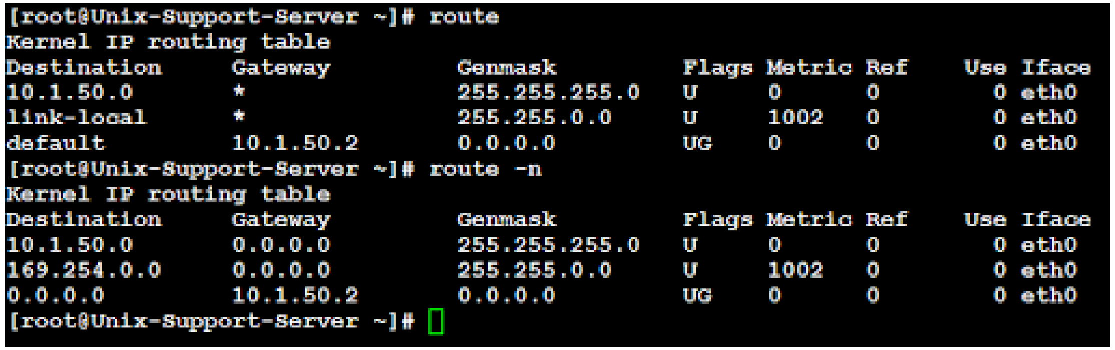
# Objective 1.05

Given a destination IP address and routing table, identify a route to be used

- **Route Tables** – The routing table is built automatically, based on the current TCP/IP configuration. The computer searches the routing table for an entry that most closely matches the destination IP address.
- **Network Destination** – The network destination is used with the netmask to match the destination IP address.
- **Gateway** – The gateway address is the IP address that the local host uses to forward IP datagrams to other IP networks.
- **Interface** – The interface is the IP address that is configured on the local computer for the local network adapter that is used when an IP datagram is forwarded on the network.
- **Metric** – A metric indicates the cost of using a route, which is typically the number of hops to the IP destination.



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.86     35
         10.1.1.0    255.255.255.0         On-link         10.1.1.1    291
         10.1.1.1  255.255.255.255         On-link         10.1.1.1    291
       10.1.1.255  255.255.255.255         On-link         10.1.1.1    291
        10.1.10.0    255.255.255.0         On-link        10.1.10.1    291
        10.1.10.1  255.255.255.255         On-link        10.1.10.1    291
```



```
[root@Unix-Support-Server ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.1.50.0       *               255.255.255.0   U     0      0        0 eth0
link-local      *               255.255.0.0     U     1002   0        0 eth0
default         10.1.50.2       0.0.0.0         UG    0      0        0 eth0
[root@Unix-Support-Server ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.1.50.0       0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         10.1.50.2       0.0.0.0         UG    0      0        0 eth0
[root@Unix-Support-Server ~]# 
```

**The BIG-IP system contains two sets of routing tables:**

The **Linux** routing tables, for routing administrative traffic through the management interface

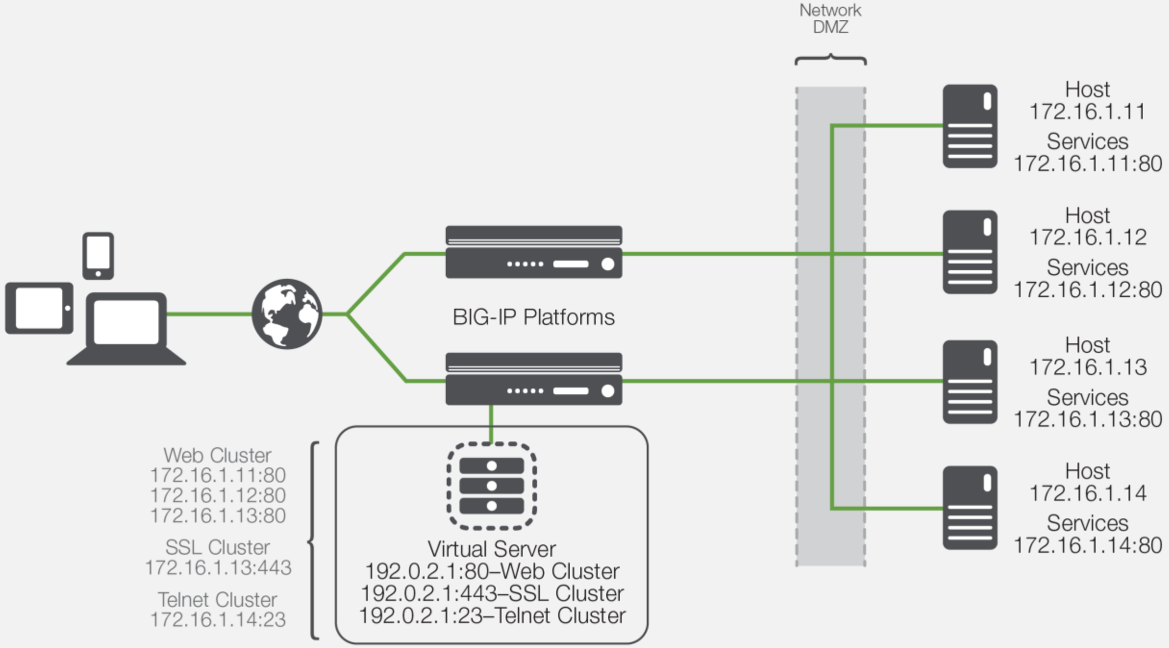
A special **TMM** routing table, for routing application and administrative traffic through the TMM interfaces

# Objective 1.06

## Define ADC application objects

### Object Definitions

- A ***node*** is a logical object on the BIG-IP® system that identifies the IP address of a physical resource on the network.
- A ***pool*** is a logical set of devices, such as web servers, that you group together to receive and process traffic
- A ***pool member*** consists of a server's IP address and service port number. An example of a pool member is 10.10.10.1:80
- A ***virtual server*** is a traffic-management object on the BIG-IP system that is represented by a virtual IP address and a service, such as 192.168.20.10:80



**Manual: BIG-IP Local. Traffic Management: Basics**

[https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0.html](https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0.html)

# Objective 1.06

## Define load balancing including intelligent load balancing and server selection

**Distribution of Load** – The distribution of inbound requests and processing of load responses across a group of servers.

A **Load balancing method** is an algorithm or formula that the BIG-IP system uses to determine the server to which traffic will be sent.

- Default load balancing method - Round Robin

**K42275060: Load-Balancing Methods** - [https://my.f5.com/manage/s/article/K42275060](https://my.f5.com/manage/s/article/K42275060)

**Round Robin –** The system passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced.

**Ratio –** The number of connections that each machine receives over time is proportionate to a ratio weight you define for each machine within the pool.

**Fastest –** The system passes a new connection based on the fastest response of all pools of which a server is a member.

**Least Connections –** The system passes a new connection to the node that has the least number of current connections out of all pools of which a node is a member.

**Weighted Least Connections –** The system uses the value you specify in Connection Limit to establish a proportional algorithm for each pool member. The system bases the load balancing decision on that proportion and the number of current connections to that pool member.

**Observed –** The system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections.

**Predictive –** Uses the ranking method used by the Observed (member) methods, except that the system analyzes the trend of the ranking over time, determining whether a node's performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections.

**Least Sessions –** The system passes a new connection to the node that currently has the least number of persistent sessions.

**Ratio Least Connections –** The system selects the pool member according to the ratio of the number of connections each pool member has active.

# Objective 1.06

Explain features of an application delivery controller

A common misconception is that an Application Delivery Controller (ADC) is an advanced load-balancer. This is not an adequate description.

An ADC is a network device that helps applications to direct user traffic in order to remove the excess load from two or more servers.

In fact, an ADC includes many OSI layer 3-7 services which happen to include load-balancing. Other features commonly found in most ADCs include SSL offload, Web Application Firewall, NAT64, DNS64, and proxy/reverse proxy to name a few.

They also tend to offer more advanced features such as content redirection as well as server health monitoring.

F5 FIREWALL, F5 LOAD BALANCER, F5 DNS
F5 DDOS PROTECTION, F5 NAT
memegenerator.net

# Objective 1.06

## Explain benefits of an application delivery controller

**Efficiency** – An application delivery controller (ADC) can improve the efficiency of the servers for which it manages application requests.

**Performance** – Application performance can be improved with features like compression, caching, protocol optimizations, connection management and intelligent load-balancing algorithms.

**Reliability** – An ADC provides reliability by ensuring that requests are sent only to available servers, redirecting requests when a server is down for maintenance or is unresponsive

**Security** – Protect applications with DDoS protection, rate limiting, blacklisting, whitelisting, authentication, resource obfuscation, SSL, content encryption and application web firewall and SSL VPN.

**Capacity** – In order to architect a solution that uses a pool of servers and balance requests across them to increase capacity, throughput and support more users.

**Scalability** – With an ADC you can add more servers to scale up as demand increases without downtime or impact.

# Section 2: Troubleshooting

# Objective 2.01

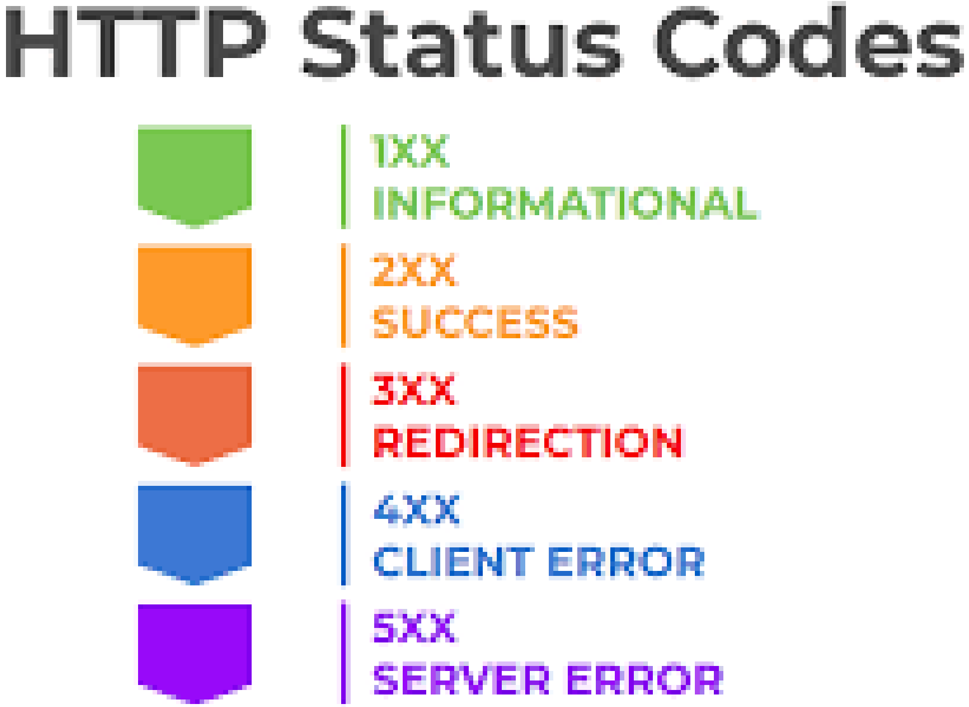
Identify application and network errors

- Identify general meanings of HTTP error codes
- Identify possible reasons and methods for connection termination
- Identify possible causes for failure to establish connection

# Objective 2.01

## Identify application and network errors

- Identify general meanings of HTTP error codes



HTTP Status Codes

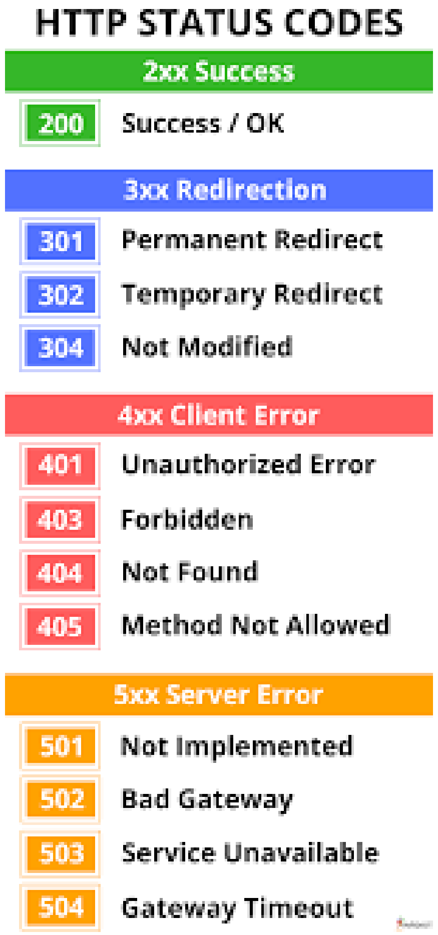
1XX INFORMATIONAL

2XX SUCCESS

3XX REDIRECTION

4XX CLIENT ERROR

5XX SERVER ERROR



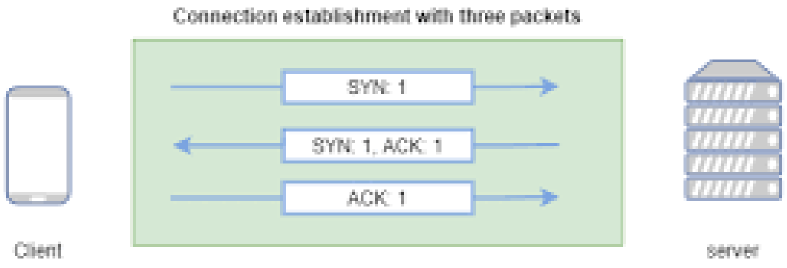
HTTP STATUS CODES

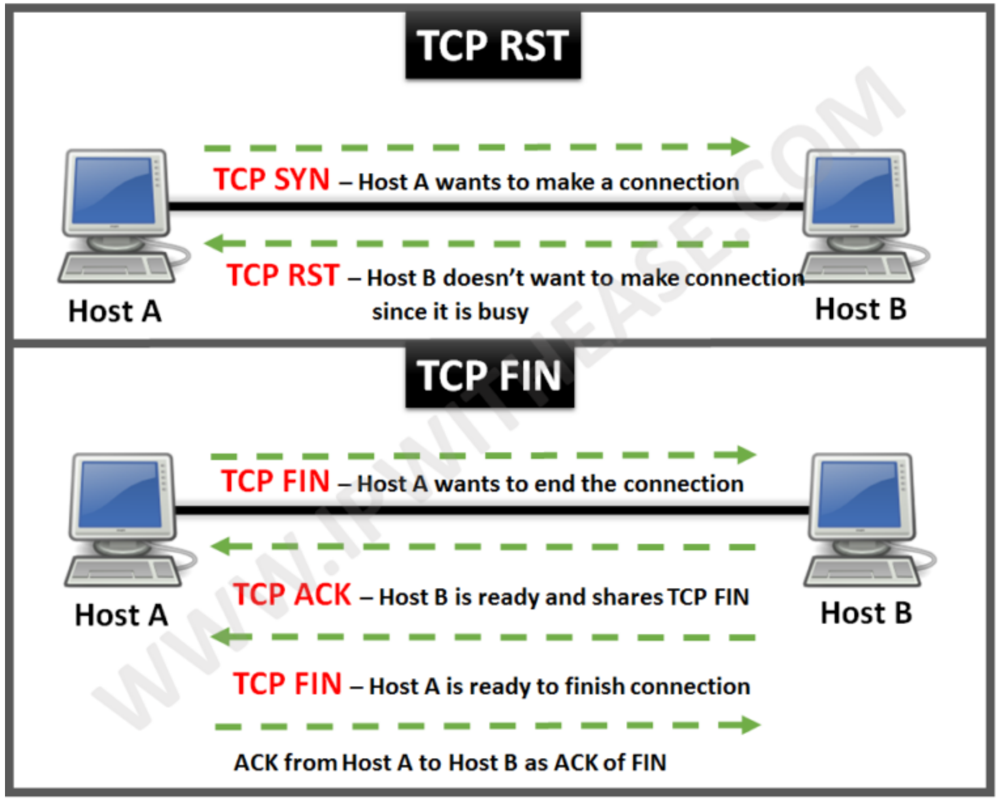
| | |
|---|---|
| 2xx Success | |
| 200 | Success / OK |
| 3xx Redirection | |
| 301 | Permanent Redirect |
| 302 | Temporary Redirect |
| 304 | Not Modified |
| 4xx Client Error | |
| 401 | Unauthorized Error |
| 403 | Forbidden |
| 404 | Not Found |
| 405 | Method Not Allowed |
| 5xx Server Error | |
| 501 | Not Implemented |
| 502 | Bad Gateway |
| 503 | Service Unavailable |
| 504 | Gateway Timeout |

# Objective 2.01

Identify application and network errors

- Identify possible reasons and methods for connection termination

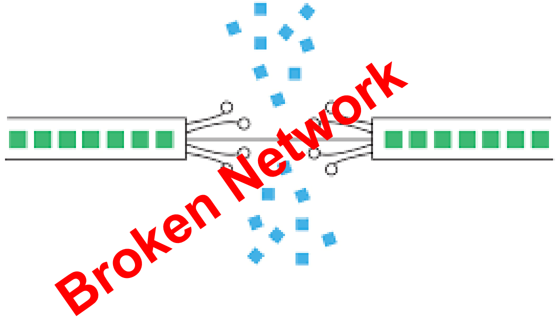



TCP RST
TCP SYN – Host A wants to make a connection
TCP RST – Host B doesn't want to make connection since it is busy
Host A
Host B
TCP FIN
TCP FIN – Host A wants to end the connection
TCP ACK – Host B is ready and shares TCP FIN
TCP FIN – Host A is ready to finish connection
ACK from Host A to Host B as ACK of FIN
Host A
Host B
WWW.IPWITHEASE.COM

# Objective 2.01

## Identify application and network errors

- Identify possible causes for failure to establish connection


Broken Network

Wrong URL

| Service | Number |
|---|---|
| FTP data | 20 |
| FTP CMD | 21 |
| SSH | 22 |
| SMTP | 25 |
| DNS | 53 |
| HTTP | 80 |
| Kerberos | 88 |
| NTP | 123 |
| SNMP | 161 |
| LDAP | 389 |
| HTTPS | 443 |
| Syslog | 514 |
| iQuery | 4353 |

Wrong Port

# Objective 2.01

Given a scenario, verify Layer 2 mapping (ARP)

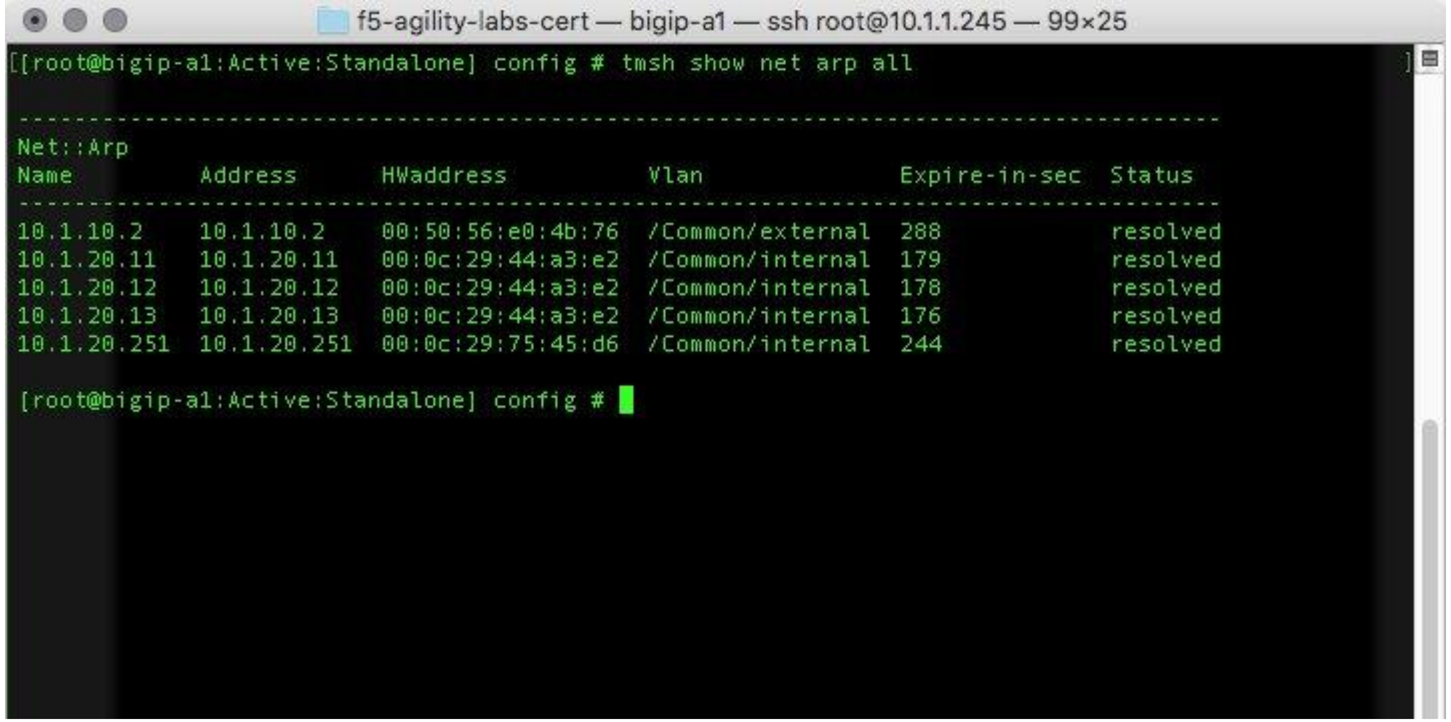
- Explain one-to-one mapping of MAC to IP
- Given a network diagram or ARP command output, determine if ARP resolution was successful
- Explain the purpose of MAC masquerading

# Objective 2.02

Given a scenario, verify Layer 2 mapping (ARP)

- Explain one-to-one mapping of MAC to IP
  - [root@bigip-a1:Active:Standalone] config # tmsh show net arp all

- Troubleshooting ARP
  - RESOLVED
  - INCOMPLETE
  - DOWN

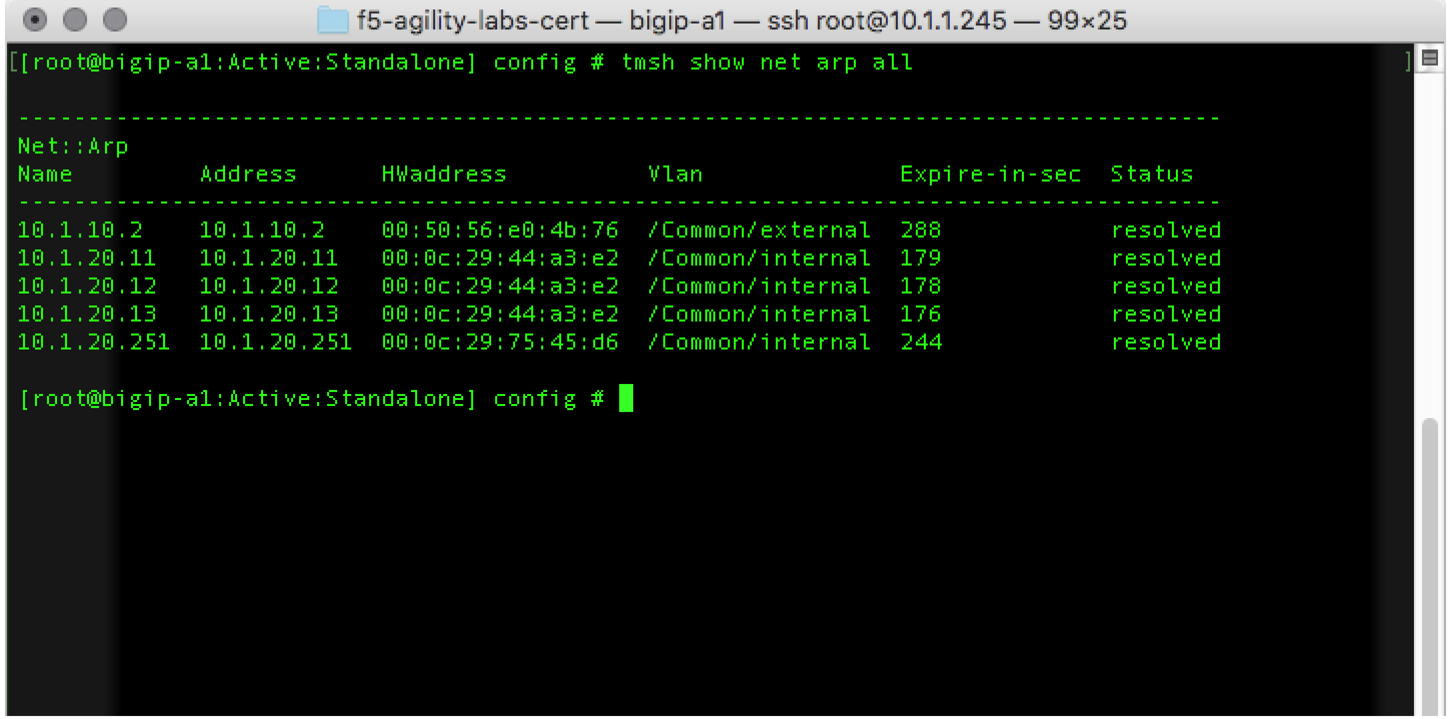

f5-agility-labs-cert — bigip-a1 — ssh root@10.1.1.245 — 99×25

```
[[root@bigip-a1:Active:Standalone] config # tmsh show net arp all

--------------------------------------------------------------------------------------
Net::Arp
Name         Address      HWaddress          Vlan              Expire-in-sec  Status
--------------------------------------------------------------------------------------
10.1.10.2    10.1.10.2    00:50:56:e0:4b:76  /Common/external  288            resolved
10.1.20.11   10.1.20.11   00:0c:29:44:a3:e2  /Common/internal  179            resolved
10.1.20.12   10.1.20.12   00:0c:29:44:a3:e2  /Common/internal  178            resolved
10.1.20.13   10.1.20.13   00:0c:29:44:a3:e2  /Common/internal  176            resolved
10.1.20.251  10.1.20.251  00:0c:29:75:45:d6  /Common/internal  244            resolved

[root@bigip-a1:Active:Standalone] config #
```

# Objective 2.02

Given a scenario, verify Layer 2 mapping (ARP)

- Given the ARP command output, determine if ARP resolution was successful
  - ARP resolution
  - [root@bigip-a1:Active:Standalone] config # tmsh show net arp all



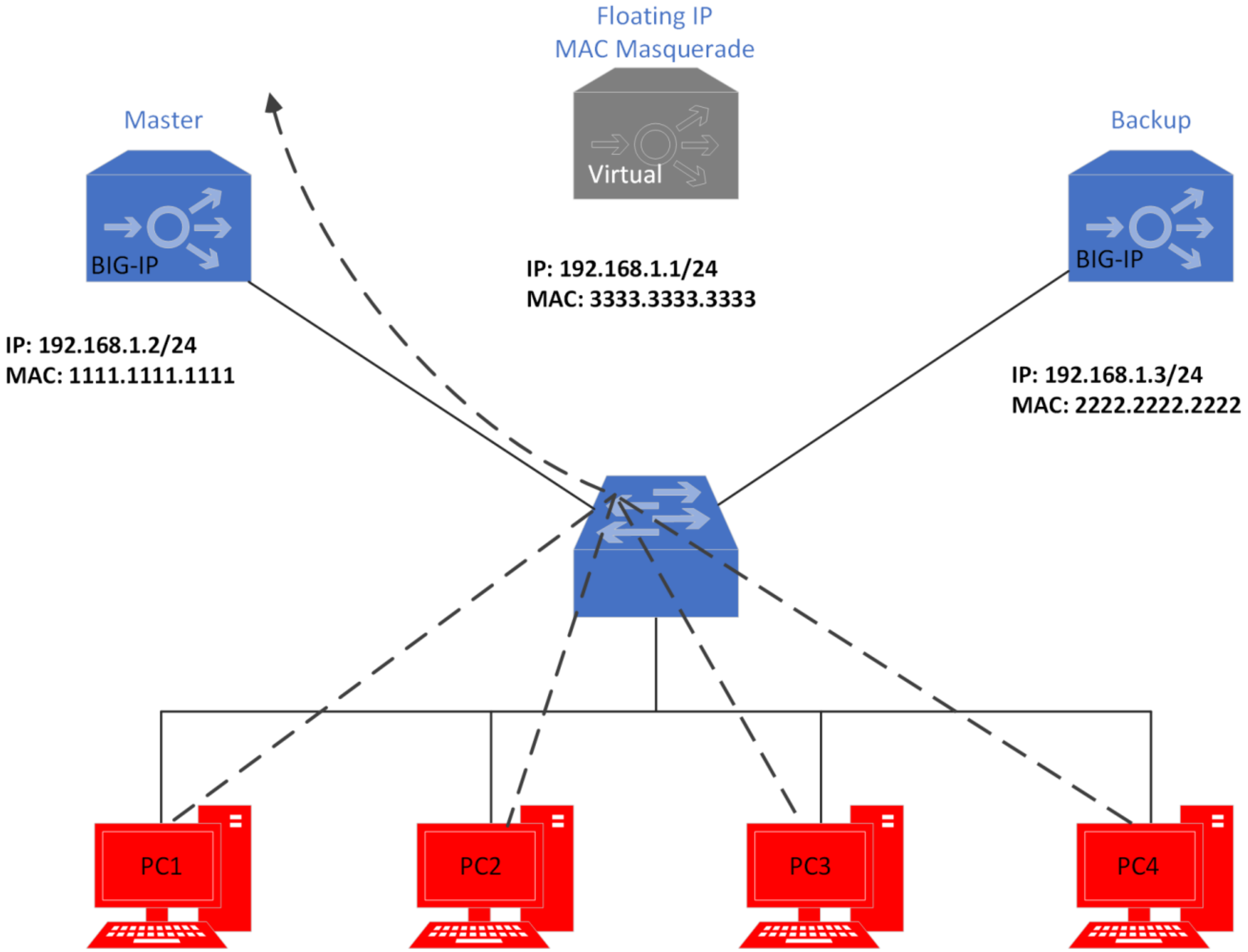
f5-agility-labs-cert — bigip-a1 — ssh root@10.1.1.245 — 99×25

```
[[root@bigip-a1:Active:Standalone] config # tmsh show net arp all

 ---------------------------------------------------------------------------------------
 Net::Arp
 Name         Address      HWaddress          Vlan              Expire-in-sec  Status
 ---------------------------------------------------------------------------------------
 10.1.10.2    10.1.10.2    00:50:56:e0:4b:76  /Common/external  288            resolved
 10.1.20.11   10.1.20.11   00:0c:29:44:a3:e2  /Common/internal  179            resolved
 10.1.20.12   10.1.20.12   00:0c:29:44:a3:e2  /Common/internal  178            resolved
 10.1.20.13   10.1.20.13   00:0c:29:44:a3:e2  /Common/internal  176            resolved
 10.1.20.251  10.1.20.251  00:0c:29:75:45:d6  /Common/internal  244            resolved

 [root@bigip-a1:Active:Standalone] config #
```

# Objective 2.02

Given a scenario, verify Layer 2 mapping (ARP)

- Explain the purpose of MAC masquerading



# Objective 2.03

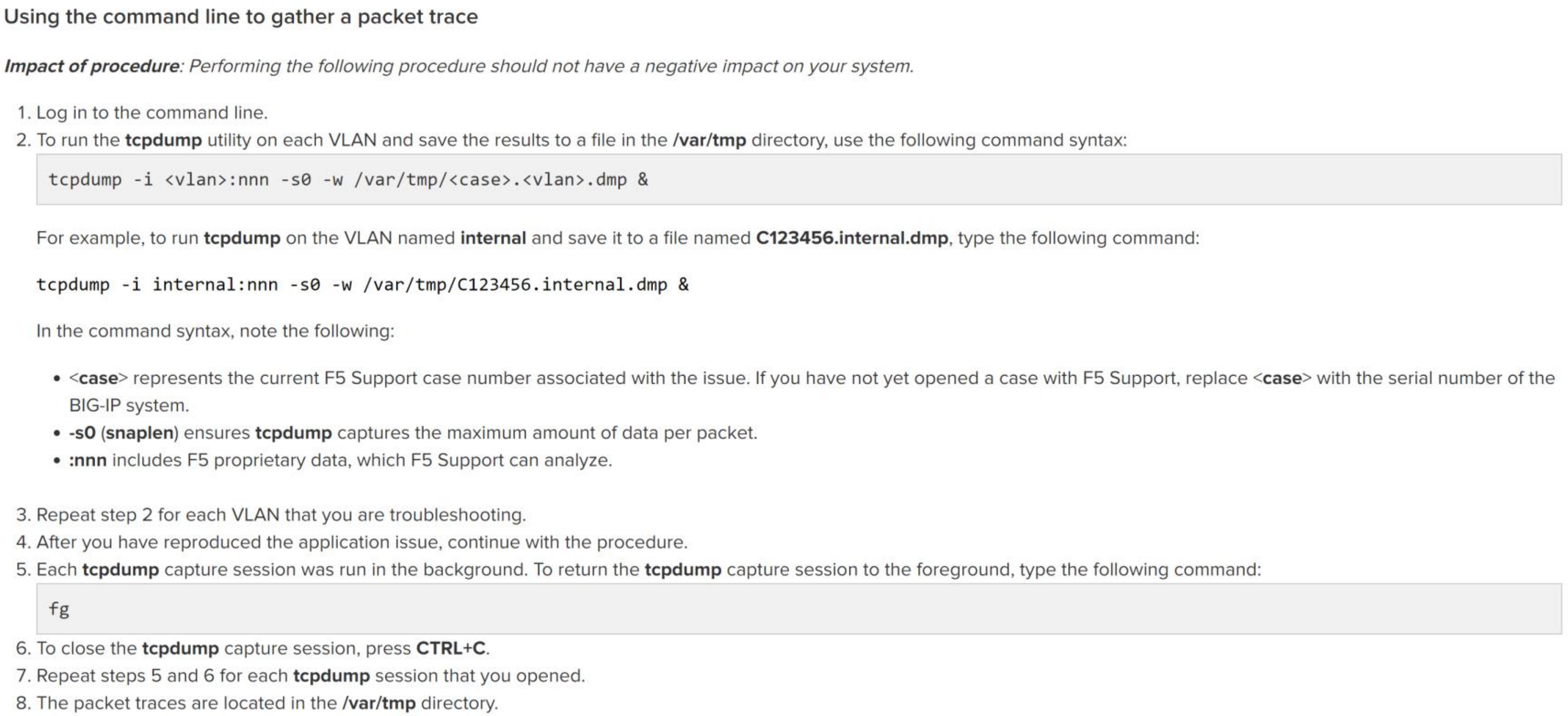
Given a scenario, verify traffic is arriving at a destination

- Explain how to acquire packet captures
- View a packet capture and identify source and destination
- Interpret statistics to show traffic flow

# Objective 2.03

Given a scenario, verify traffic is arriving at a destination

- Explain how to acquire packet captures
- TCPDUMP
- TMUI Caputre



### Using the command line to gather a packet trace

***Impact of procedure**: Performing the following procedure should not have a negative impact on your system.*

1. Log in to the command line.
2. To run the **tcpdump** utility on each VLAN and save the results to a file in the **/var/tmp** directory, use the following command syntax:

   ```
   tcpdump -i <vlan>:nnn -s0 -w /var/tmp/<case>.<vlan>.dmp &
   ```

   For example, to run **tcpdump** on the VLAN named **internal** and save it to a file named **C123456.internal.dmp**, type the following command:

   ```
   tcpdump -i internal:nnn -s0 -w /var/tmp/C123456.internal.dmp &
   ```

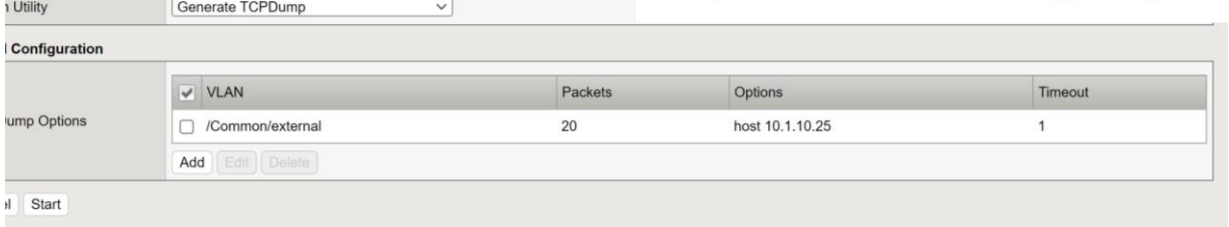
   In the command syntax, note the following:

   - <**case**> represents the current F5 Support case number associated with the issue. If you have not yet opened a case with F5 Support, replace <**case**> with the serial number of the BIG-IP system.
   - **-s0** (**snaplen**) ensures **tcpdump** captures the maximum amount of data per packet.
   - **:nnn** includes F5 proprietary data, which F5 Support can analyze.

3. Repeat step 2 for each VLAN that you are troubleshooting.
4. After you have reproduced the application issue, continue with the procedure.
5. Each **tcpdump** capture session was run in the background. To return the **tcpdump** capture session to the foreground, type the following command:

   ```
   fg
   ```

6. To close the **tcpdump** capture session, press **CTRL+C**.
7. Repeat steps 5 and 6 for each **tcpdump** session that you opened.
8. The packet traces are located in the **/var/tmp** directory.



rt Snapshot

ı Utility: Generate TCPDump

l Configuration

ump Options:

| ☑ VLAN | Packets | Options | Timeout |
|---|---|---|---|
| □ /Common/external | 20 | host 10.1.10.25 | 1 |

# Objective 2.03

Given a scenario, verify traffic is arriving at a destination

- View a packet capture and identify source and destination

## Read tcpdump binary file output

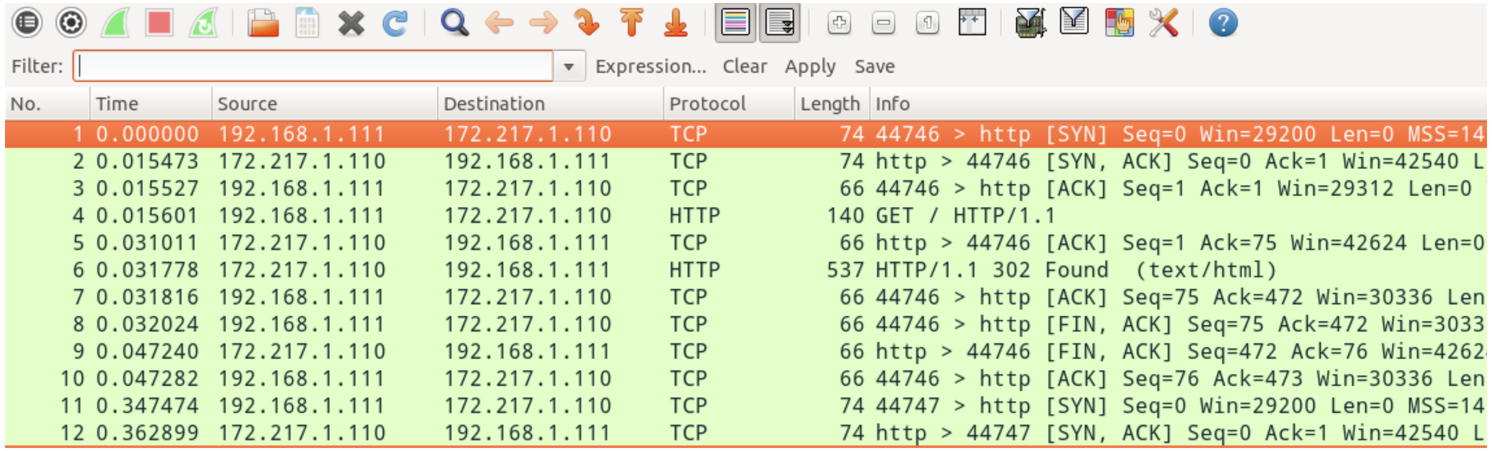
To read data from a binary **tcpdump** file (that you saved by using the **tcpdump -w** command), type the following command:

```
tcpdump -r <filename>
```

For example:

```
tcpdump -r dump1.bin
```

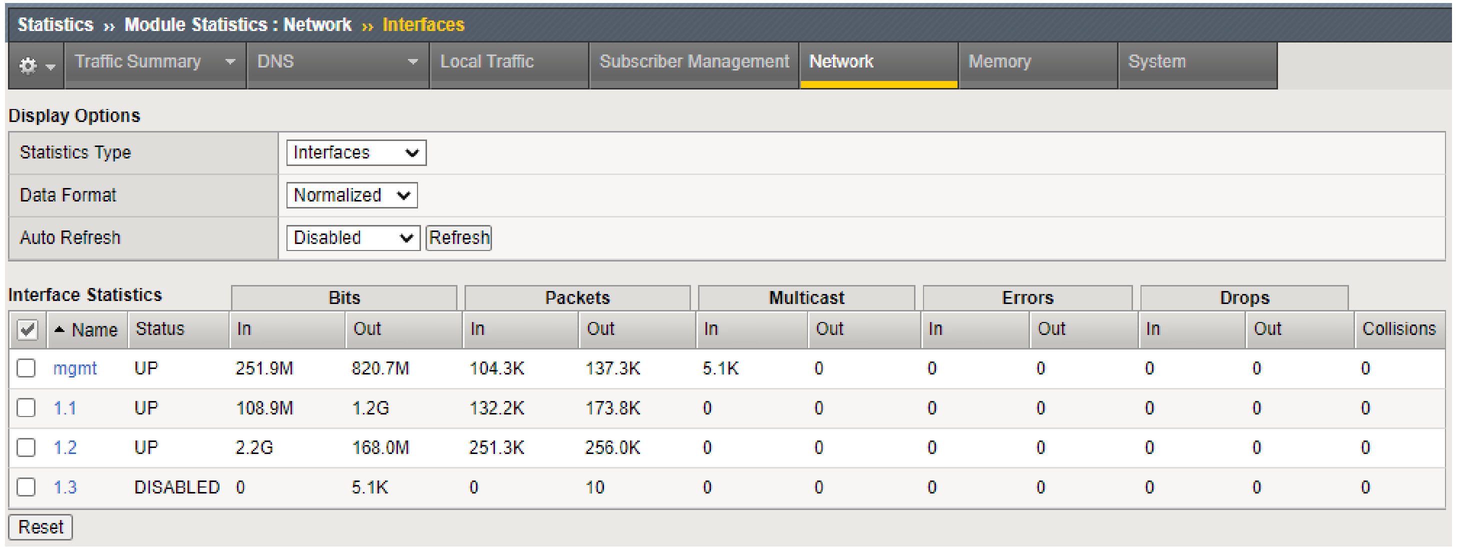
In this mode, the **tcpdump** utility reads stored packets from the file, but otherwise operates just as it would if it were reading from the network interface. As a result, you can use formatting commands and filters.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.1.111 | 172.217.1.110 | TCP | 74 | 44746 > http [SYN] Seq=0 Win=29200 Len=0 MSS=14 |
| 2 | 0.015473 | 172.217.1.110 | 192.168.1.111 | TCP | 74 | http > 44746 [SYN, ACK] Seq=0 Ack=1 Win=42540 L |
| 3 | 0.015527 | 192.168.1.111 | 172.217.1.110 | TCP | 66 | 44746 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 |
| 4 | 0.015601 | 192.168.1.111 | 172.217.1.110 | HTTP | 140 | GET / HTTP/1.1 |
| 5 | 0.031011 | 172.217.1.110 | 192.168.1.111 | TCP | 66 | http > 44746 [ACK] Seq=1 Ack=75 Win=42624 Len=0 |
| 6 | 0.031778 | 172.217.1.110 | 192.168.1.111 | HTTP | 537 | HTTP/1.1 302 Found  (text/html) |
| 7 | 0.031816 | 192.168.1.111 | 172.217.1.110 | TCP | 66 | 44746 > http [ACK] Seq=75 Ack=472 Win=30336 Len |
| 8 | 0.032024 | 192.168.1.111 | 172.217.1.110 | TCP | 66 | 44746 > http [FIN, ACK] Seq=75 Ack=472 Win=3033 |
| 9 | 0.047240 | 172.217.1.110 | 192.168.1.111 | TCP | 66 | http > 44746 [FIN, ACK] Seq=472 Ack=76 Win=4262 |
| 10 | 0.047282 | 192.168.1.111 | 172.217.1.110 | TCP | 66 | 44746 > http [ACK] Seq=76 Ack=473 Win=30336 Len |
| 11 | 0.347474 | 192.168.1.111 | 172.217.1.110 | TCP | 74 | 44747 > http [SYN] Seq=0 Win=29200 Len=0 MSS=14 |
| 12 | 0.362899 | 172.217.1.110 | 192.168.1.111 | TCP | 74 | http > 44747 [SYN, ACK] Seq=0 Ack=1 Win=42540 L |

# Objective 2.03

Given a scenario, verify traffic is arriving at a destination



Display Options

| | |
|---|---|
| Statistics Type | Interfaces |
| Data Format | Normalized |
| Auto Refresh | Disabled Refresh |

Interface Statistics

| | | | Bits | | Packets | | Multicast | | Errors | | Drops | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ▲ Name | Status | In | Out | In | Out | In | Out | In | Out | In | Out | Collisions |
| □ | mgmt | UP | 251.9M | 820.7M | 104.3K | 137.3K | 5.1K | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.1 | UP | 108.9M | 1.2G | 132.2K | 173.8K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.2 | UP | 2.2G | 168.0M | 251.3K | 256.0K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.3 | DISABLED | 0 | 5.1K | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Reset

- Errors – number of packets containing errors
- Drops – number of packets drop for processing or packet errors
- Collisions – should only occur on half-duplex

```
(tmos)# show net interface
----------------------------------------------------------------------
Net::Interface
Name    Status    Bits    Bits    Pkts    Pkts  Drops  Errs      Media
                    In     Out      In     Out

----------------------------------------------------------------------
1.1         up  111.4M    1.3G  136.1K  178.7K      0     0  10000T-FD
1.2         up    2.2G  170.3M  256.0K  260.3K      0     0  10000T-FD
1.3   disabled       0    5.1K       0      10      0     0       none
mgmt        up  254.3M  831.2M  105.4K  139.0K      0     0   100TX-FD
```

# Objective 2.04

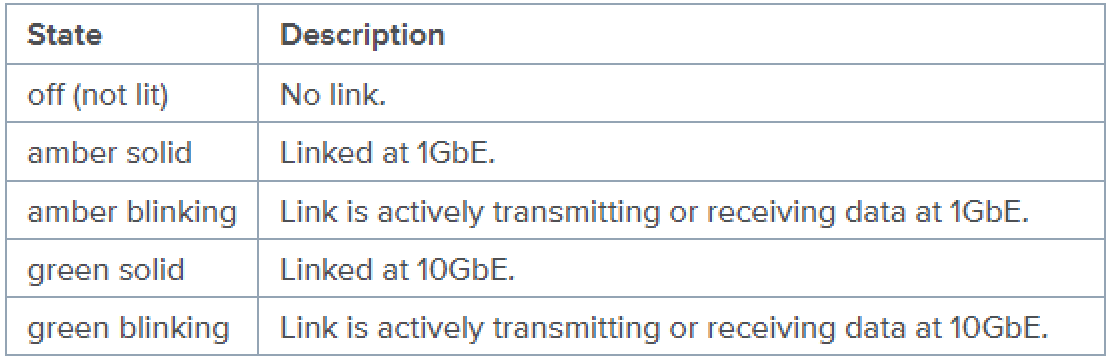
Given a scenario, verify Layer 1 connectivity

- Given an exhibit of the front ethernet panel, explain why there is an imbalance in link use
- Interpret ifconfig ouput (interface bandwidth)
- Explain potential L1 failure modes (duplex settings, cable out of specification)

# Objective 2.04

## Given a scenario, verify Layer 1 connectivity

- Given an exhibit of the front ethernet panel, explain why there is an imbalance in link use
  - https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/platform-i2000-i4000/1.html#guid-0f2cb19a-9ff1-4583-9f0a-0f3c2cc04a88
  - Front Panel Link Status

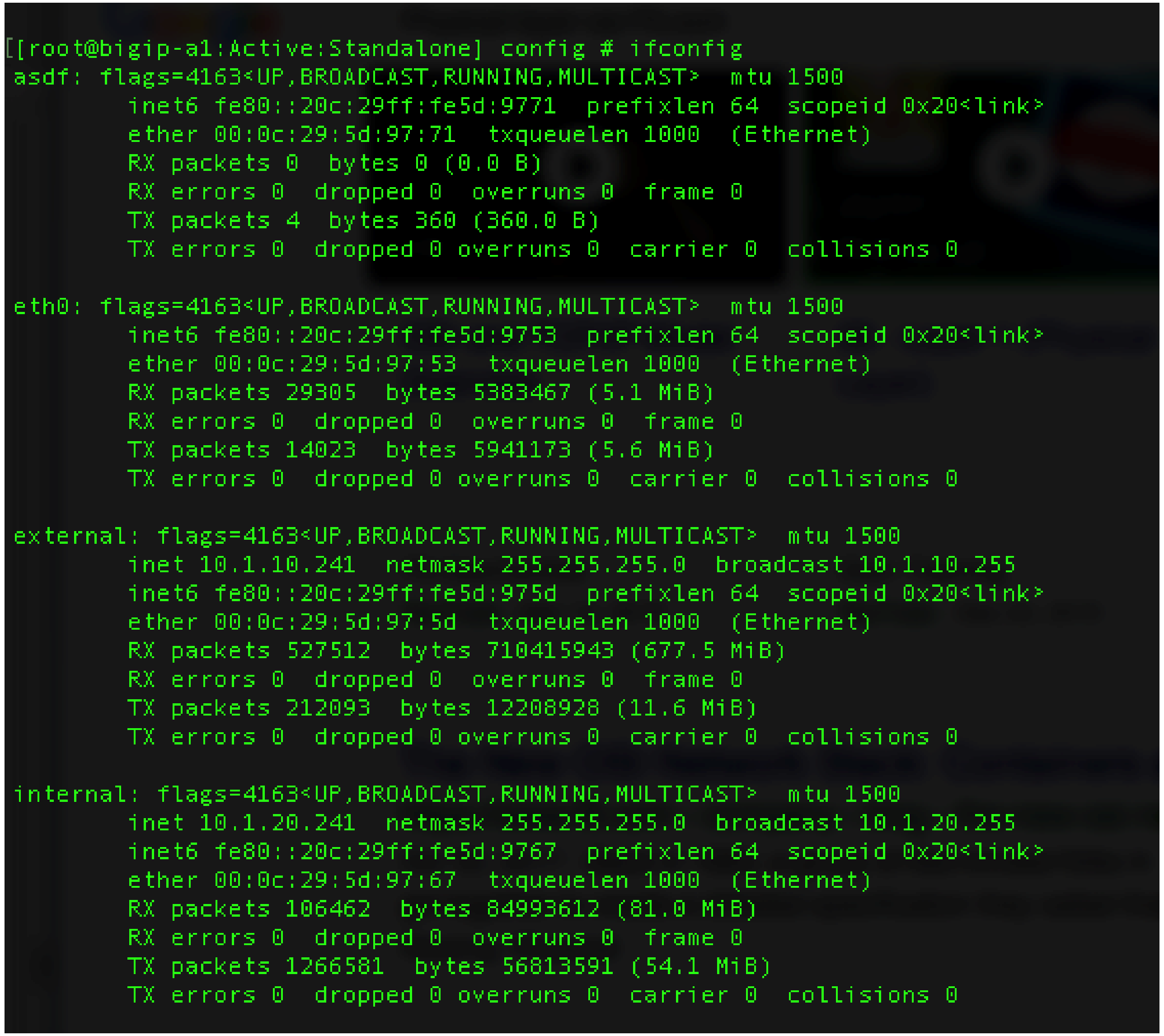


| State | Description |
|---|---|
| off (not lit) | No link. |
| amber solid | Linked at 1GbE. |
| amber blinking | Link is actively transmitting or receiving data at 1GbE. |
| green solid | Linked at 10GbE. |
| green blinking | Link is actively transmitting or receiving data at 10GbE. |

# Objective 2.04

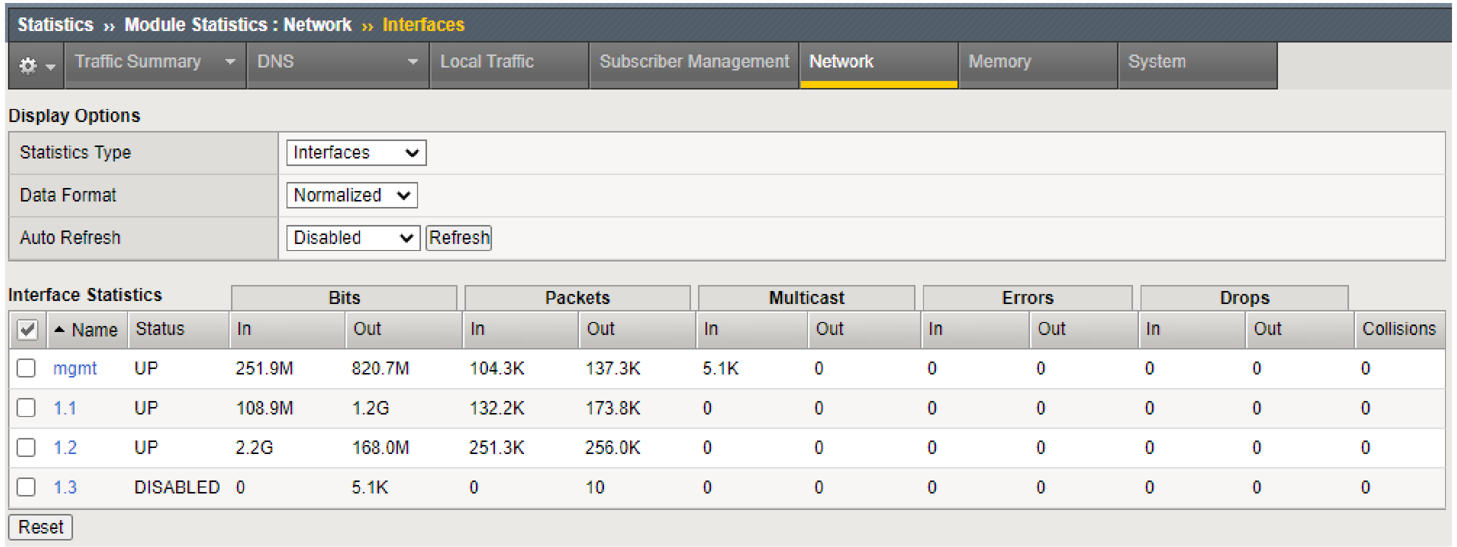
Given a scenario, verify Layer 1 connectivity

- Interpret ifconfig output (interface bandwidth)
  - https://en.wikipedia.org/wiki/Ifconfig
  - Ifconfig output



```
[[root@bigip-a1:Active:Standalone] config # ifconfig
 asdf: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe5d:9771  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:97:71  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 360 (360.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe5d:9753  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:97:53  txqueuelen 1000  (Ethernet)
        RX packets 29305  bytes 5383467 (5.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14023  bytes 5941173 (5.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

 external: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.10.241  netmask 255.255.255.0  broadcast 10.1.10.255
        inet6 fe80::20c:29ff:fe5d:975d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:97:5d  txqueuelen 1000  (Ethernet)
        RX packets 527512  bytes 710415943 (677.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 212093  bytes 12208928 (11.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

 internal: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.20.241  netmask 255.255.255.0  broadcast 10.1.20.255
        inet6 fe80::20c:29ff:fe5d:9767  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:97:67  txqueuelen 1000  (Ethernet)
        RX packets 106462  bytes 84993612 (81.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1266581  bytes 56813591 (54.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

# Identify when drops are occurring



Display Options

| | |
|---|---|
| Statistics Type | Interfaces |
| Data Format | Normalized |
| Auto Refresh | Disabled Refresh |

Interface Statistics

| | | | Bits | | Packets | | Multicast | | Errors | | Drops | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Name | Status | In | Out | In | Out | In | Out | In | Out | In | Out | Collisions |
| □ | mgmt | UP | 251.9M | 820.7M | 104.3K | 137.3K | 5.1K | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.1 | UP | 108.9M | 1.2G | 132.2K | 173.8K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.2 | UP | 2.2G | 168.0M | 251.3K | 256.0K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.3 | DISABLED | 0 | 5.1K | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Reset

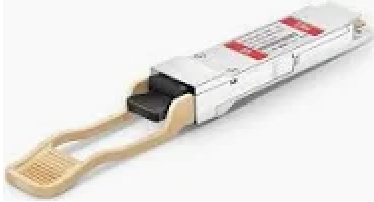
- Errors – number of packets containing errors
- Drops – number of packets drop for processing or packet errors
- Collisions – should only occur on half-duplex

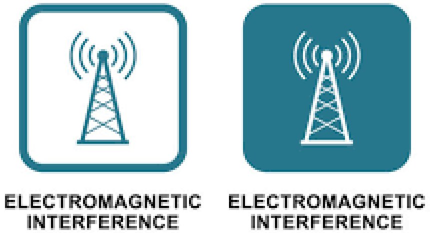
```
(tmos)# show net interface
----------------------------------------------------------------------
Net::Interface
Name    Status    Bits    Bits    Pkts    Pkts  Drops  Errs      Media
                    In     Out      In     Out
----------------------------------------------------------------------
1.1         up  111.4M    1.3G  136.1K  178.7K      0     0  10000T-FD
1.2         up    2.2G  170.3M  256.0K  260.3K      0     0  10000T-FD
1.3   disabled       0    5.1K       0      10      0     0       none
mgmt        up  254.3M  831.2M  105.4K  139.0K      0     0   100TX-FD
```

# Objective 2.04

Given a scenario, verify Layer 1 connectivity

- Explain potential L1 failure modes (duplex settings, cable out of specification)
  - Physical Layer (Layer 1) Failures



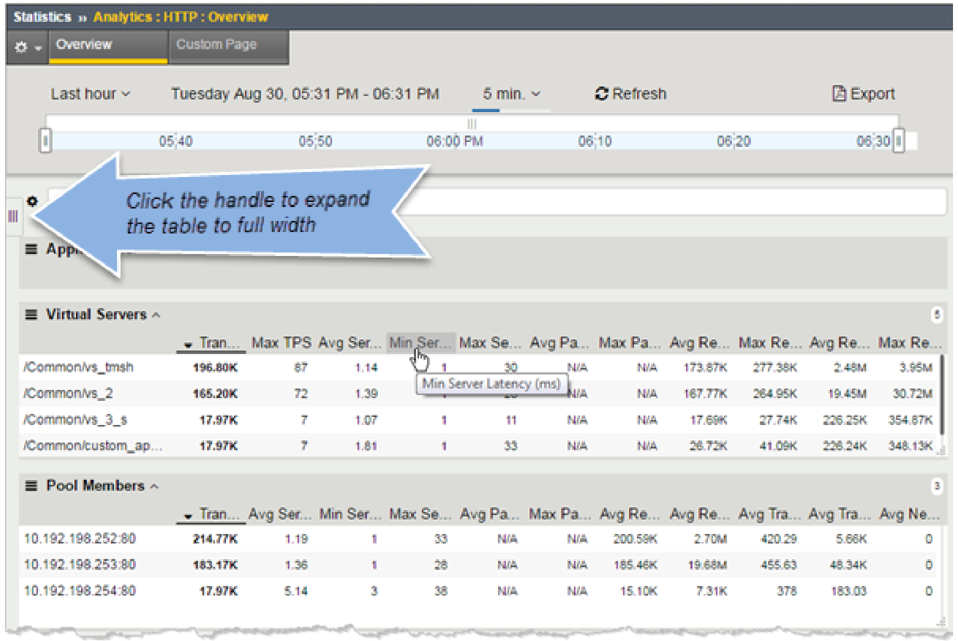


# Section 3: Maintenance

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

## Interpret traffic object statistics



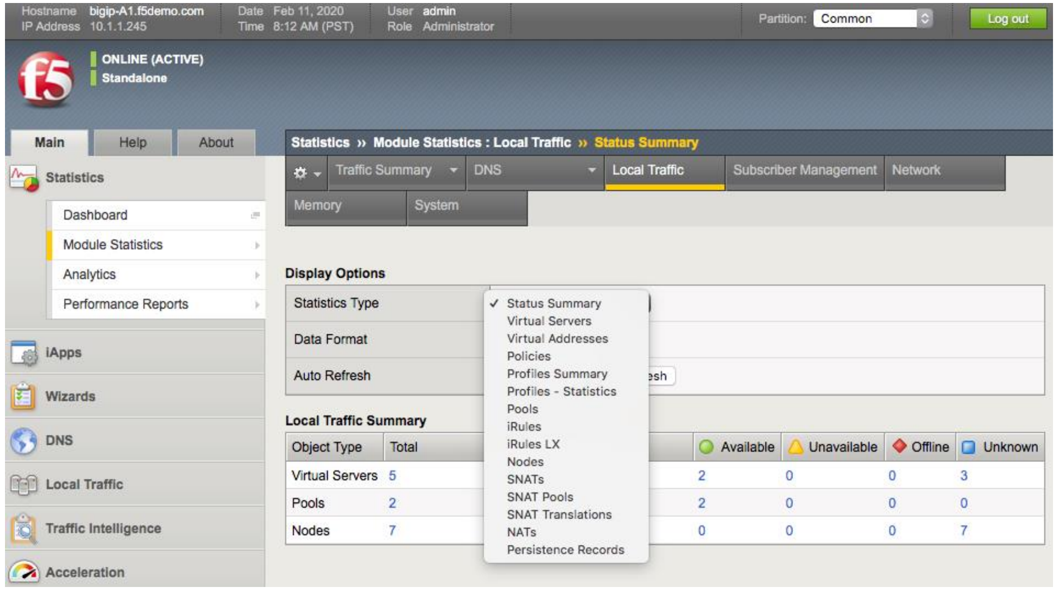
*Click the handle to expand the table to full width*

**Virtual Servers** 5

| | Tran... | Max TPS | Avg Ser... | Min Ser... | Max Se... | Avg Pa... | Max Pa... | Avg Re... | Max Re... | Avg Re... | Max Re... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| /Common/vs_tmsh | 196.80K | 87 | 1.14 | 1 | 30 | N/A | N/A | 173.87K | 277.38K | 2.48M | 3.95M |
| /Common/vs_2 | 165.20K | 72 | 1.39 | [illegible] | [illegible] | N/A | N/A | 167.77K | 264.95K | 19.45M | 30.72M |
| /Common/vs_3_s | 17.97K | 7 | 1.07 | 1 | 11 | N/A | N/A | 17.69K | 27.74K | 226.25K | 354.87K |
| /Common/custom_ap... | 17.97K | 7 | 1.81 | 1 | 33 | N/A | N/A | 26.72K | 41.09K | 226.24K | 348.13K |

**Pool Members** 3

| | Tran... | Avg Ser... | Min Ser... | Max Se... | Avg Pa... | Max Pa... | Avg Re... | Avg Re... | Avg Tra... | Avg Tra... | Avg Ne... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.192.198.252:80 | 214.77K | 1.19 | 1 | 33 | N/A | N/A | 200.59K | 2.70M | 420.29 | 5.66K | 0 |
| 10.192.198.253:80 | 183.17K | 1.36 | 1 | 28 | N/A | N/A | 185.46K | 19.68M | 455.63 | 48.34K | 0 |
| 10.192.198.254:80 | 17.97K | 5.14 | 3 | 38 | N/A | N/A | 15.10K | 7.31K | 378 | 183.03 | 0 |

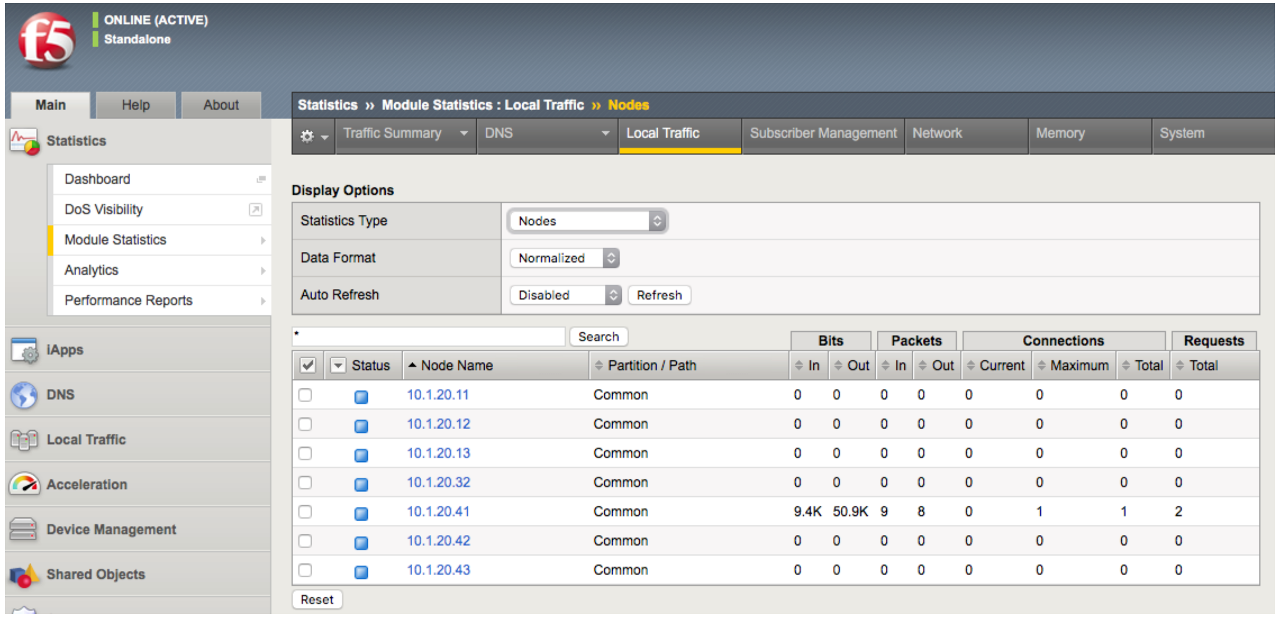


**Display Options**

| | |
|---|---|
| Statistics Type | Status Summary |
| Data Format | |
| Auto Refresh | |

**Local Traffic Summary**

| Object Type | Total | Available | Unavailable | Offline | Unknown |
|---|---|---|---|---|---|
| Virtual Servers | 5 | 2 | 0 | 0 | 3 |
| Pools | 2 | 2 | 0 | 0 | 0 |
| Nodes | 7 | 0 | 0 | 0 | 7 |



**Display Options**

| | |
|---|---|
| Statistics Type | Nodes |
| Data Format | Normalized |
| Auto Refresh | Disabled Refresh |

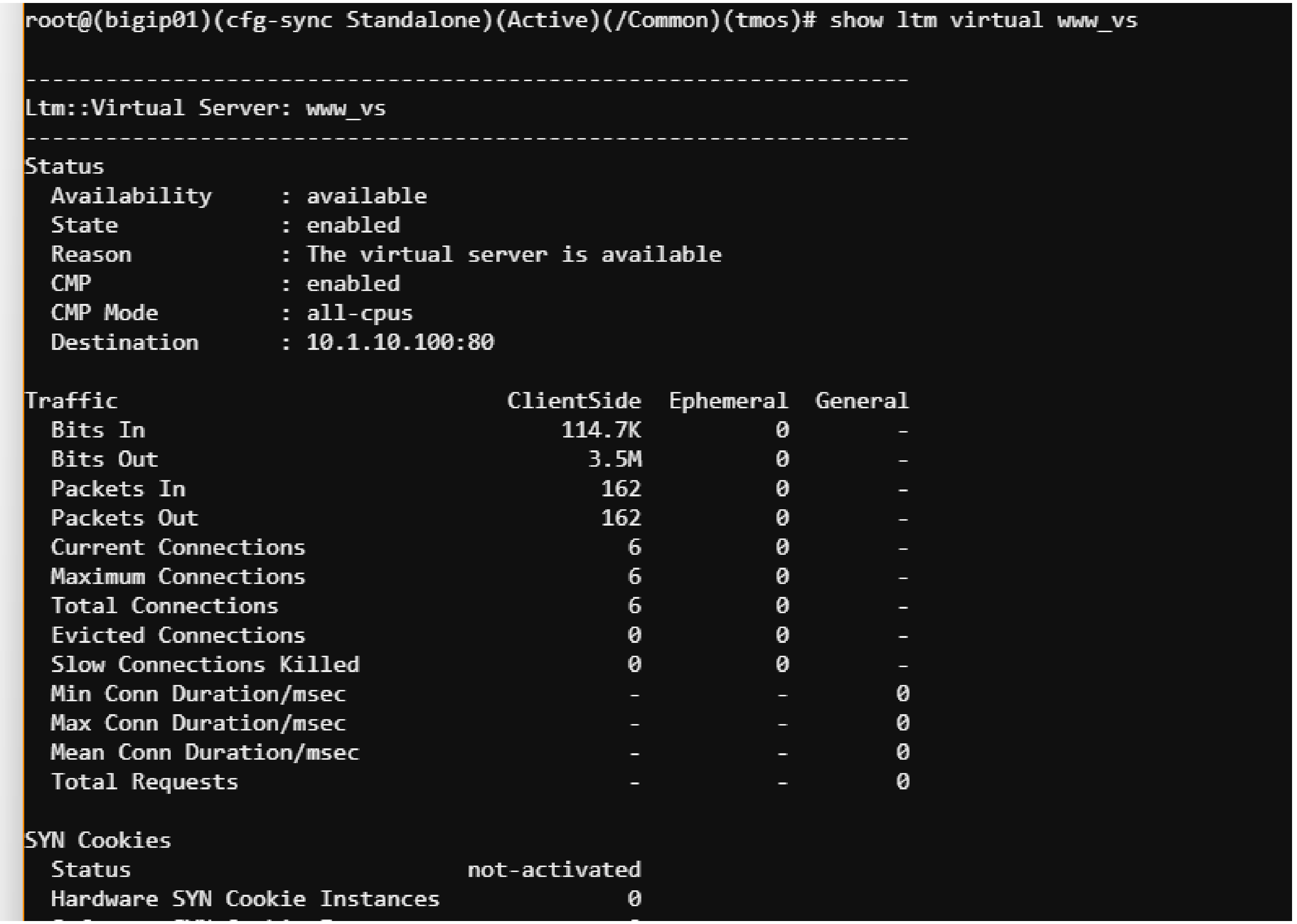
| | | | | Bits | | Packets | | Connections | | | Requests |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Status | Node Name | Partition / Path | In | Out | In | Out | Current | Maximum | Total | Total |
| □ | ■ | 10.1.20.11 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | ■ | 10.1.20.12 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | ■ | 10.1.20.13 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | ■ | 10.1.20.32 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | ■ | 10.1.20.41 | Common | 9.4K | 50.9K | 9 | 8 | 0 | 1 | 1 | 2 |
| □ | ■ | 10.1.20.42 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | ■ | 10.1.20.43 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

https://clouddocs.f5.com/cli/tmsh-reference/latest/commands/show.html

(tmos)# show ltm virtual int_www_vs

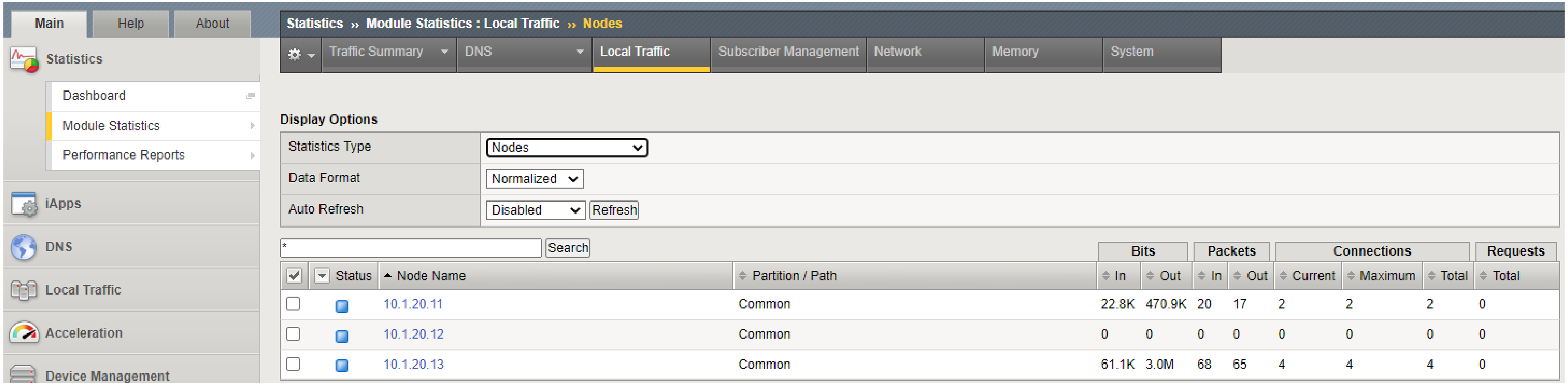


```
root@(bigip01)(cfg-sync Standalone)(Active)(/Common)(tmos)# show ltm virtual www_vs

------------------------------------------------------------------
Ltm::Virtual Server: www_vs
------------------------------------------------------------------
Status
  Availability     : available
  State            : enabled
  Reason           : The virtual server is available
  CMP              : enabled
  CMP Mode         : all-cpus
  Destination      : 10.1.10.100:80

Traffic                             ClientSide  Ephemeral  General
  Bits In                               114.7K          0        -
  Bits Out                                3.5M          0        -
  Packets In                               162          0        -
  Packets Out                              162          0        -
  Current Connections                        6          0        -
  Maximum Connections                        6          0        -
  Total Connections                          6          0        -
  Evicted Connections                        0          0        -
  Slow Connections Killed                    0          0        -
  Min Conn Duration/msec                     -          -        0
  Max Conn Duration/msec                     -          -        0
  Mean Conn Duration/msec                    -          -        0
  Total Requests                             -          -        0

SYN Cookies
  Status                         not-activated
  Hardware SYN Cookie Instances              0
```

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

## Nodes screenshot



Display Options

| | |
|---|---|
| Statistics Type | Nodes |
| Data Format | Normalized |
| Auto Refresh | Disabled [Refresh] |

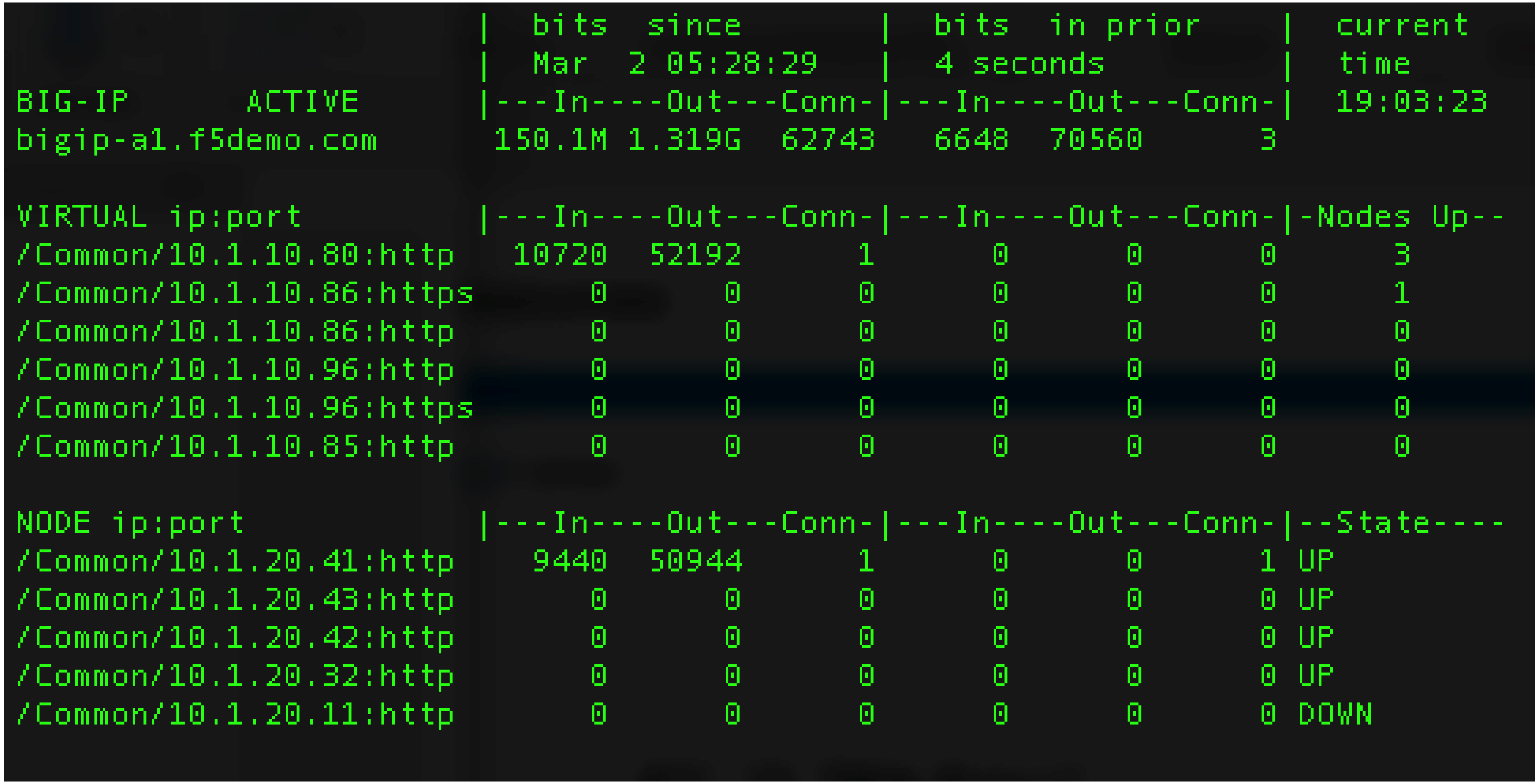
* [Search]

| | | | | Bits | | Packets | | Connections | | | Requests |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Status | Node Name | Partition / Path | In | Out | In | Out | Current | Maximum | Total | Total |
| □ | 🟦 | 10.1.20.11 | Common | 22.8K | 470.9K | 20 | 17 | 2 | 2 | 2 | 0 |
| □ | 🟦 | 10.1.20.12 | Common | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 🟦 | 10.1.20.13 | Common | 61.1K | 3.0M | 68 | 65 | 4 | 4 | 4 | 0 |

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

[root@bigip-a1:Active:Standalone] config # bigtop

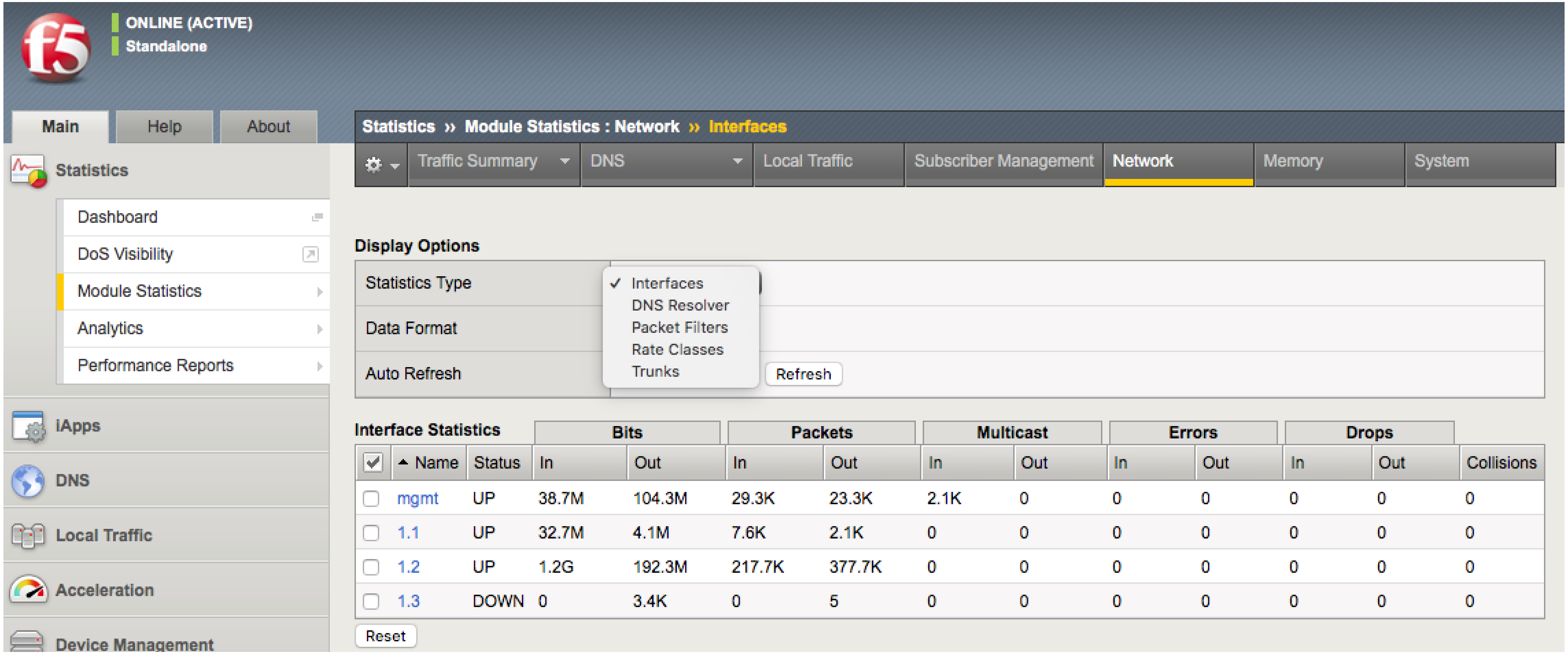


```
                        |  bits  since       |  bits  in prior    |  current
                        |  Mar  2 05:28:29   |  4 seconds         |  time
BIG-IP      ACTIVE      |---In----Out---Conn-|---In----Out---Conn-|  19:03:23
bigip-a1.f5demo.com      150.1M 1.319G  62743   6648  70560      3

VIRTUAL ip:port         |---In----Out---Conn-|---In----Out---Conn-|-Nodes Up--
/Common/10.1.10.80:http   10720  52192      1      0      0      0      3
/Common/10.1.10.86:https      0      0      0      0      0      0      1
/Common/10.1.10.86:http       0      0      0      0      0      0      0
/Common/10.1.10.96:http       0      0      0      0      0      0      0
/Common/10.1.10.96:https      0      0      0      0      0      0      0
/Common/10.1.10.85:http       0      0      0      0      0      0      0

NODE ip:port            |---In----Out---Conn-|---In----Out---Conn-|--State----
/Common/10.1.20.41:http    9440  50944      1      0      0      1 UP
/Common/10.1.20.43:http       0      0      0      0      0      0 UP
/Common/10.1.20.42:http       0      0      0      0      0      0 UP
/Common/10.1.20.32:http       0      0      0      0      0      0 UP
/Common/10.1.20.11:http       0      0      0      0      0      0 DOWN
```

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

## Interpret network configuration statistics



Display Options

Statistics Type: Interfaces

Data Format

Auto Refresh

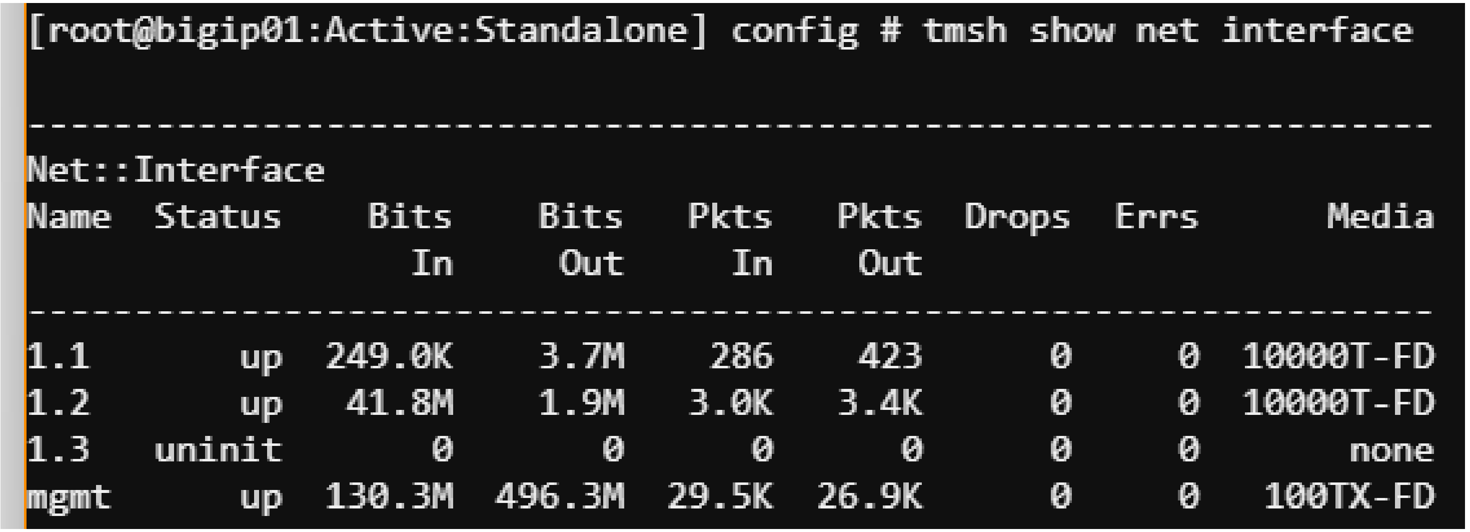
Interface Statistics

| ☑ | Name | Status | Bits In | Bits Out | Packets In | Packets Out | Multicast In | Multicast Out | Errors In | Errors Out | Drops In | Drops Out | Collisions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | mgmt | UP | 38.7M | 104.3M | 29.3K | 23.3K | 2.1K | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.1 | UP | 32.7M | 4.1M | 7.6K | 2.1K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.2 | UP | 1.2G | 192.3M | 217.7K | 377.7K | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| □ | 1.3 | DOWN | 0 | 3.4K | 0 | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Objective 3.01

Given a scenario, review basic stats to confirm functionality

config # tmsh show net interface



```
[root@bigip01:Active:Standalone] config # tmsh show net interface

-------------------------------------------------------------------
Net::Interface
Name  Status    Bits     Bits    Pkts    Pkts  Drops  Errs     Media
                  In      Out      In     Out
-------------------------------------------------------------------
1.1       up  249.0K     3.7M     286     423      0     0  10000T-FD
1.2       up   41.8M     1.9M    3.0K    3.4K      0     0  10000T-FD
1.3   uninit       0        0       0       0      0     0       none
mgmt      up  130.3M   496.3M   29.5K   26.9K      0     0   100TX-FD
```

# Objective 3.02

Given a scenario, determine device upgrade eligibility

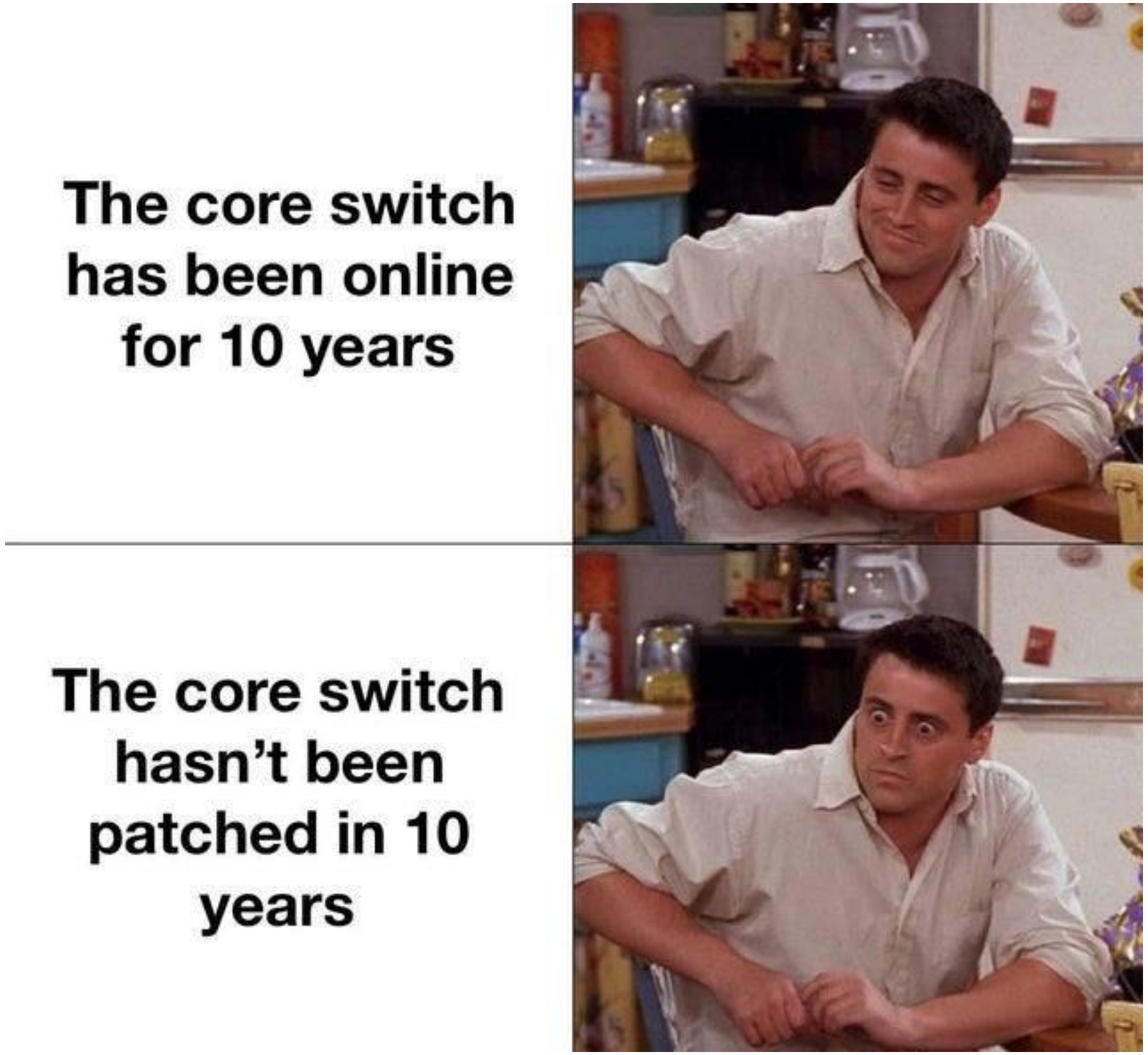
**Determine when to upgrade software**

- New features, long term support, CVEs, bug fixes…
- The F5 hardware/software compatibility matrix

**K13845: Overview of supported BIG-IP upgrade paths and an upgrade planning reference**
https://support.f5.com/csp/article/K13845

**Manual : BIG-IP Systems: Upgrading Software**
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-upgrading-software-13-0-0.html

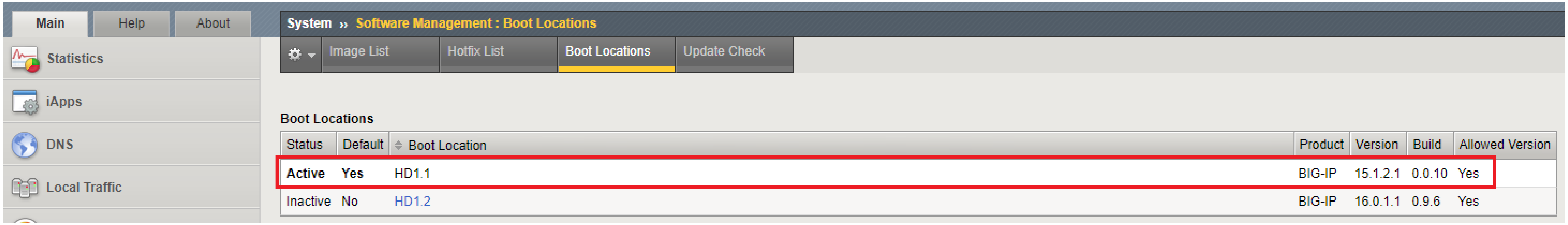
**K99014642: Choose a BIG-IP update or upgrade version | BIG-IP update and upgrade guide**
https://my.f5.com/manage/s/article/K99014642


The core switch has been online for 10 years
The core switch hasn’t been patched in 10 years

# Objective 3.02

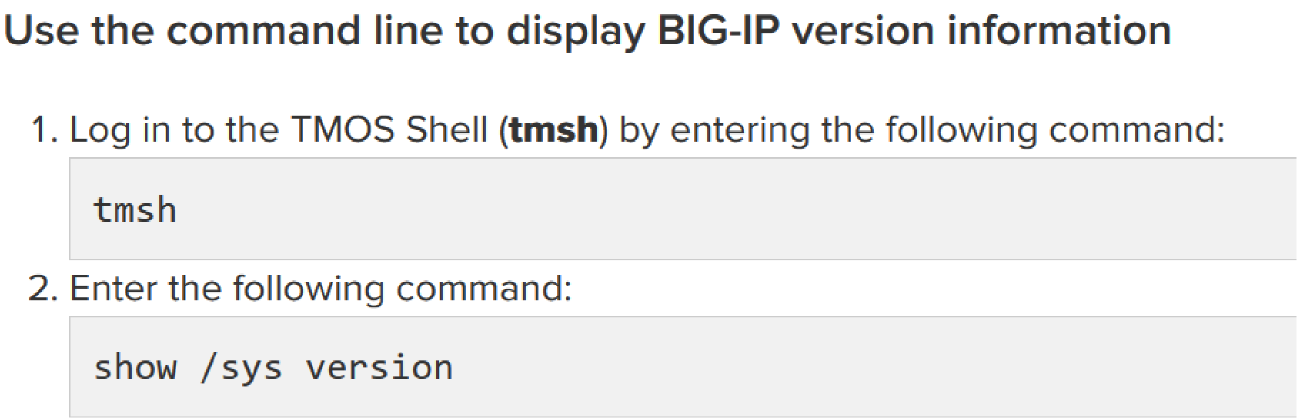
Given a scenario, determine device upgrade eligibility

### What software version is it running?



Boot Locations

| Status | Default | Boot Location | Product | Version | Build | Allowed Version |
|---|---|---|---|---|---|---|
| **Active** | **Yes** | HD1.1 | BIG-IP | 15.1.2.1 | 0.0.10 | Yes |
| Inactive | No | HD1.2 | BIG-IP | 16.0.1.1 | 0.9.6 | Yes |



## Use the command line to display BIG-IP version information

1. Log in to the TMOS Shell (**tmsh**) by entering the following command:

```
tmsh
```

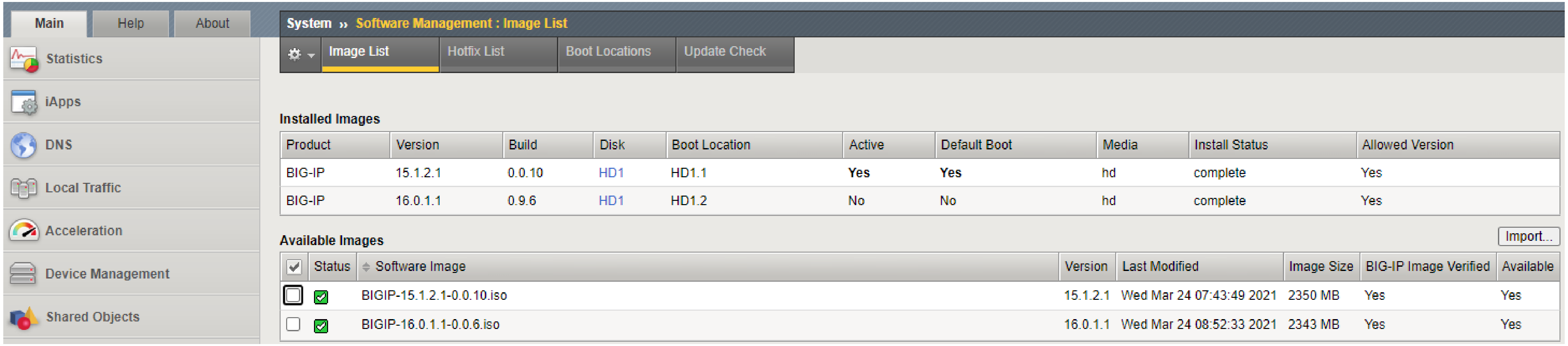
2. Enter the following command:

```
show /sys version
```

# Objective 3.02

Given a scenario, determine device upgrade eligibility

## Software inventory



Installed Images

| Product | Version | Build | Disk | Boot Location | Active | Default Boot | Media | Install Status | Allowed Version |
|---|---|---|---|---|---|---|---|---|---|
| BIG-IP | 15.1.2.1 | 0.0.10 | HD1 | HD1.1 | **Yes** | **Yes** | hd | complete | Yes |
| BIG-IP | 16.0.1.1 | 0.9.6 | HD1 | HD1.2 | No | No | hd | complete | Yes |

Available Images

| ☑ | Status | Software Image | Version | Last Modified | Image Size | BIG-IP Image Verified | Available |
|---|---|---|---|---|---|---|---|
| □ | ✓ | BIGIP-15.1.2.1-0.0.10.iso | 15.1.2.1 | Wed Mar 24 07:43:49 2021 | 2350 MB | Yes | Yes |
| □ | ✓ | BIGIP-16.0.1.1-0.0.6.iso | 16.0.1.1 | Wed Mar 24 08:52:33 2021 | 2343 MB | Yes | Yes |

For example, the **tmsh show /sys software status** command lists the currently installed software images and the associated volumes. When listing the installed software using the **tmsh show /sys software status** command, volumes are first sorted alphabetically and then numerically:

```
---------------------------------------------------
Sys::Software Status
Volume Product Version Build Active Status
---------------------------------------------------
HD1.1 BIG-IP 11.5.2 0.0.141 no  complete
HD1.2 BIG-IP 11.5.3 0.0.163 yes complete
```

# Objective 3.02

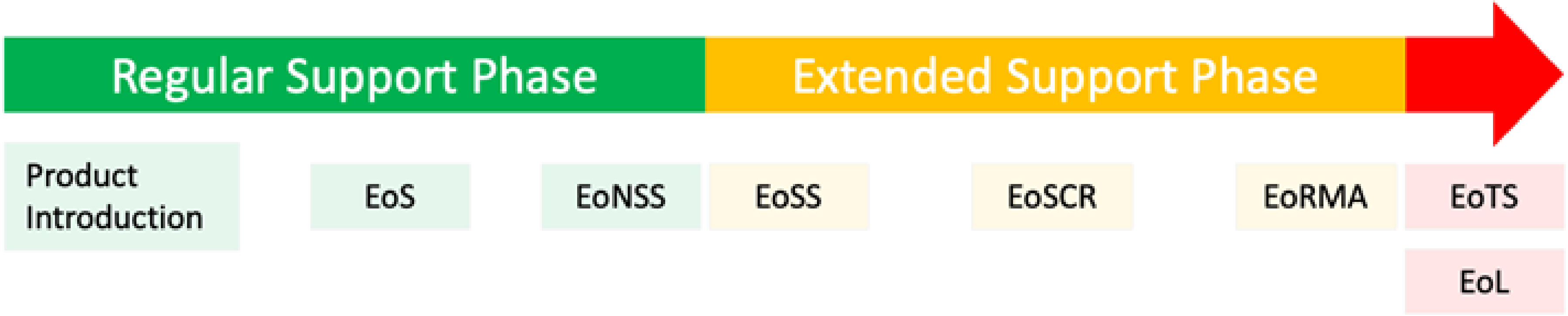
Given a scenario, determine device upgrade eligibility

**Determine when to upgrade platform**

- Platform specific features such as vCMP, PVA, SSL, FIPS, Virtual Edition
- Workload requirements
- Hardware Lifecycle - https://my.f5.com/manage/s/article/K4309
- Software Compatibility – https://my.f5.com/manage/s/article/K9476

**Hardware product support milestones**

1. Introduction: limited and general availability
2. End of Sale (EoS)
3. End of New Software Support (EoNSS)
4. End of Software Support (EoSS)
5. End of Support Contract Renewal (EoSCR)
6. End of RMA (EoRMA)
7. End of Technical Support (EoTS)
8. End of Life (EoL)

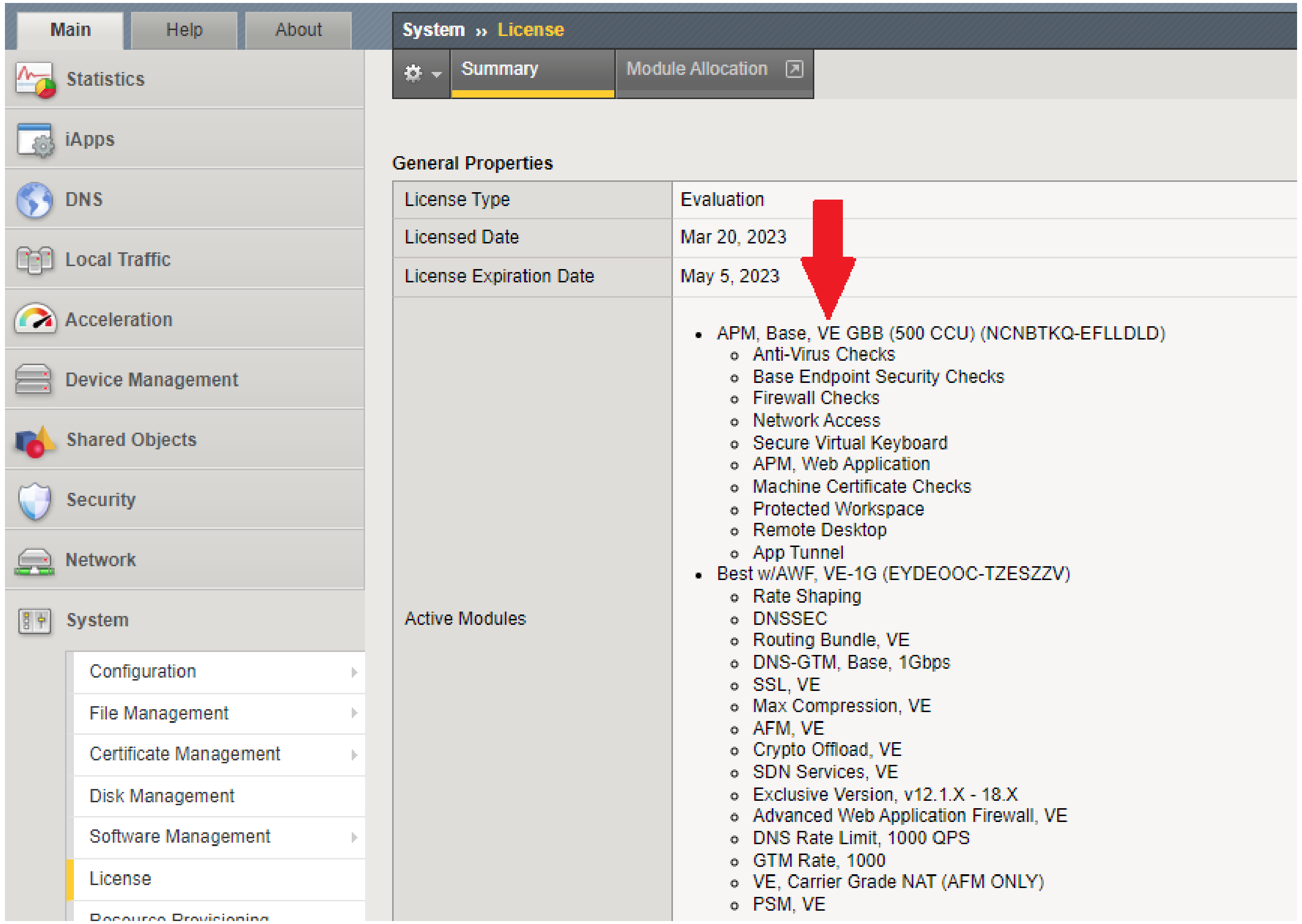


For a list of abbreviations used in the lifecycle policies, including detailed definitions, refer to K8986: F5 product support policies.

# Objective 3.02

## Given a scenario, determine device upgrade eligibility

### What platform is this device?

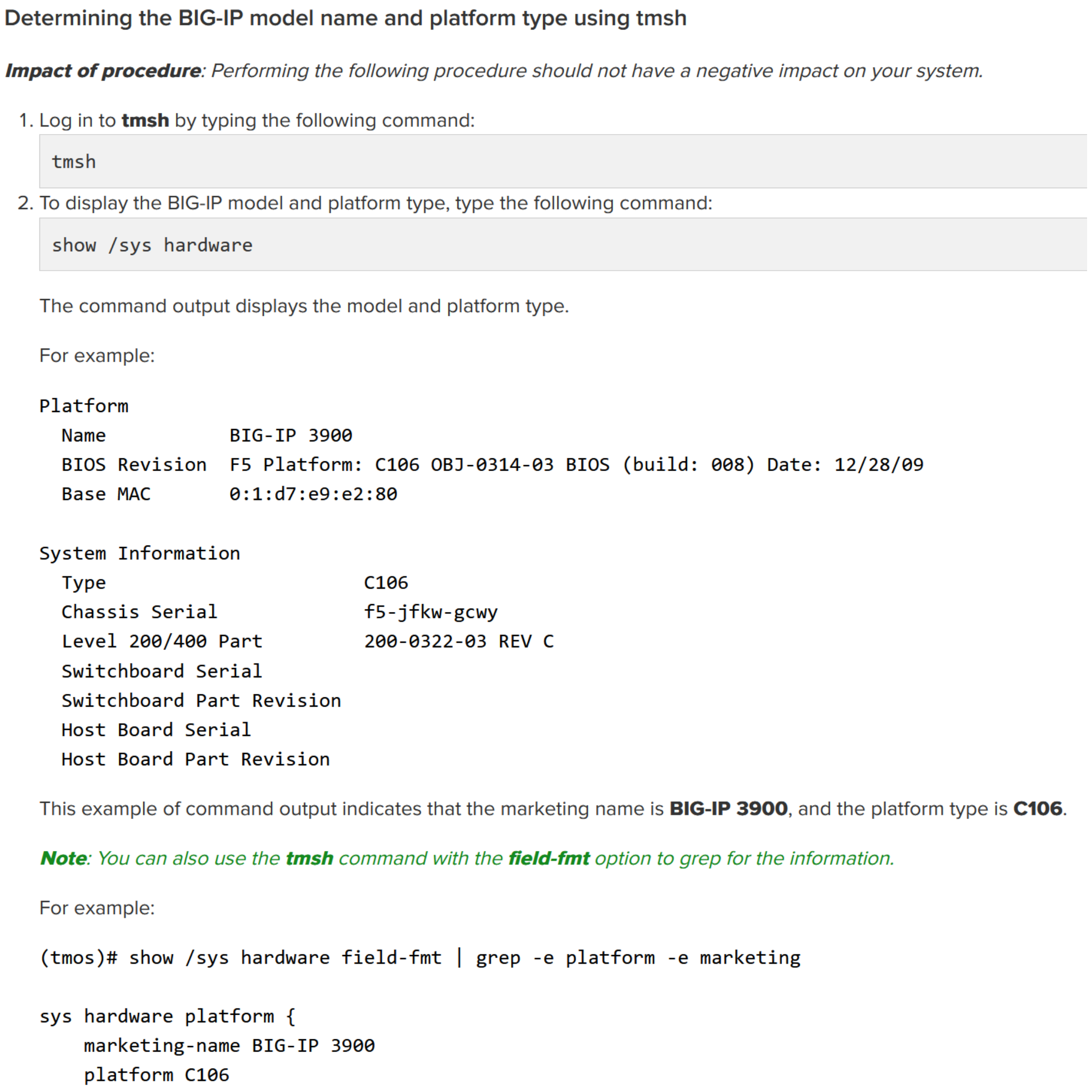


General Properties

| | |
|---|---|
| License Type | Evaluation |
| Licensed Date | Mar 20, 2023 |
| License Expiration Date | May 5, 2023 |

Active Modules

- APM, Base, VE GBB (500 CCU) (NCNBTKQ-EFLLDLD)
  - Anti-Virus Checks
  - Base Endpoint Security Checks
  - Firewall Checks
  - Network Access
  - Secure Virtual Keyboard
  - APM, Web Application
  - Machine Certificate Checks
  - Protected Workspace
  - Remote Desktop
  - App Tunnel
- Best w/AWF, VE-1G (EYDEOOC-TZESZZV)
  - Rate Shaping
  - DNSSEC
  - Routing Bundle, VE
  - DNS-GTM, Base, 1Gbps
  - SSL, VE
  - Max Compression, VE
  - AFM, VE
  - Crypto Offload, VE
  - SDN Services, VE
  - Exclusive Version, v12.1.X - 18.X
  - Advanced Web Application Firewall, VE
  - DNS Rate Limit, 1000 QPS
  - GTM Rate, 1000
  - VE, Carrier Grade NAT (AFM ONLY)
  - PSM, VE



**Determining the BIG-IP model name and platform type using tmsh**

***Impact of procedure****: Performing the following procedure should not have a negative impact on your system.*

1. Log in to **tmsh** by typing the following command:

```
tmsh
```

2. To display the BIG-IP model and platform type, type the following command:

```
show /sys hardware
```

The command output displays the model and platform type.

For example:

```
Platform
  Name            BIG-IP 3900
  BIOS Revision   F5 Platform: C106 OBJ-0314-03 BIOS (build: 008) Date: 12/28/09
  Base MAC        0:1:d7:e9:e2:80

System Information
  Type                          C106
  Chassis Serial                f5-jfkw-gcwy
  Level 200/400 Part            200-0322-03 REV C
  Switchboard Serial
  Switchboard Part Revision
  Host Board Serial
  Host Board Part Revision
```

This example of command output indicates that the marketing name is **BIG-IP 3900**, and the platform type is **C106**.

***Note****: You can also use the* ***tmsh*** *command with the* ***field-fmt*** *option to grep for the information.*

For example:

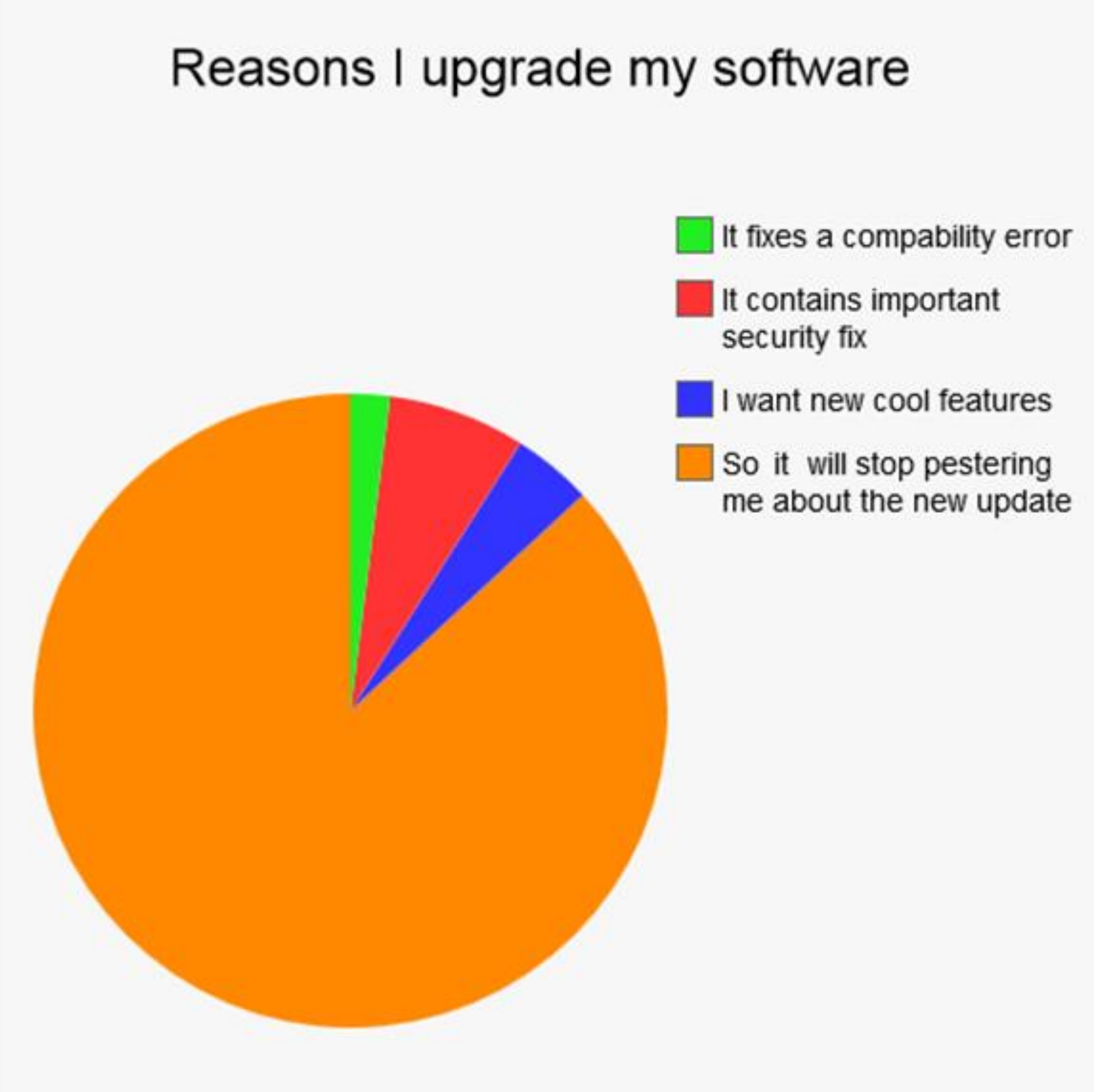
```
(tmos)# show /sys hardware field-fmt | grep -e platform -e marketing

sys hardware platform {
    marketing-name BIG-IP 3900
    platform C106
```

# Objective 3.02

Given a scenario, determine device upgrade eligibility

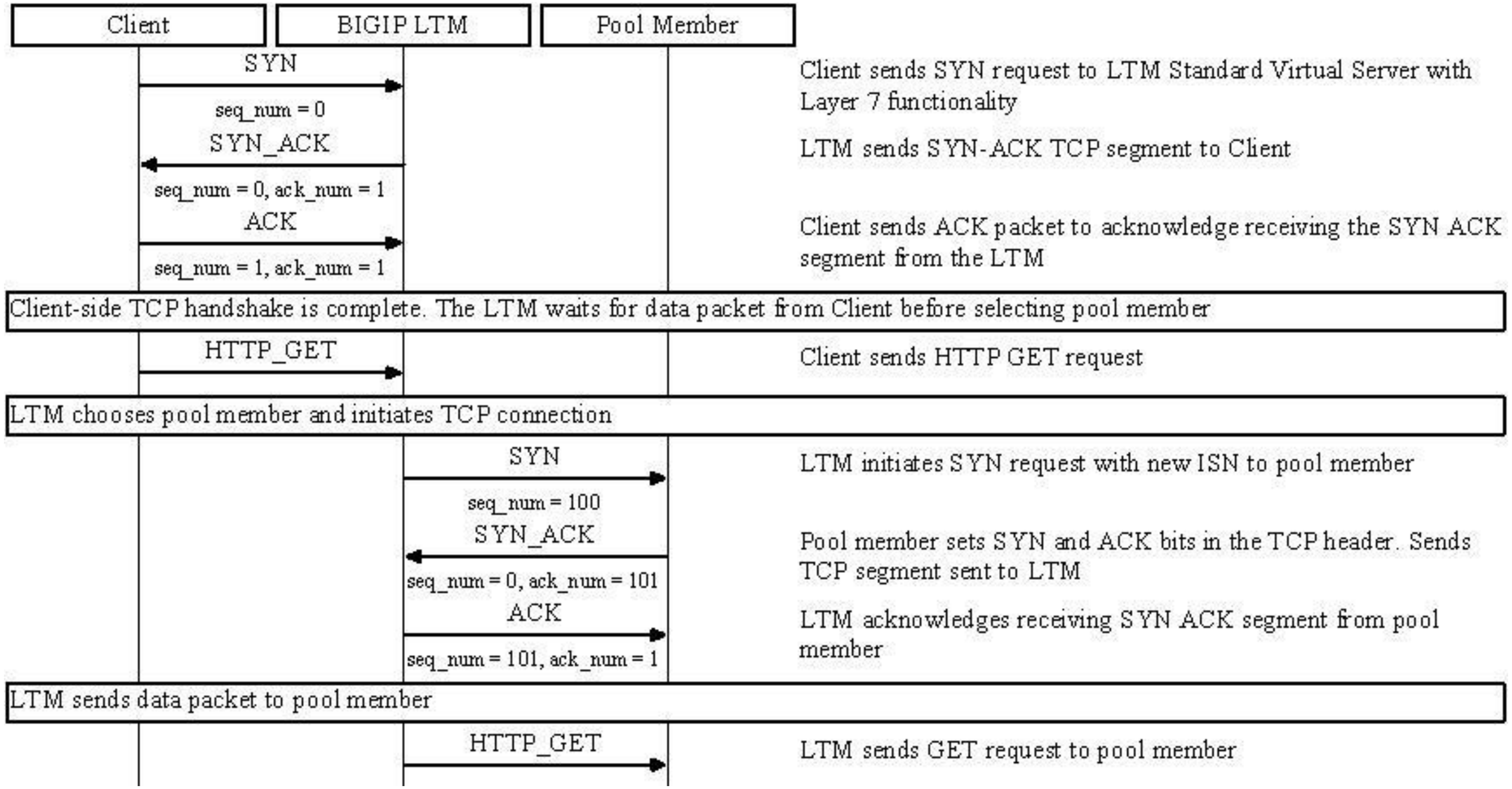
**Determine steps to minimize upgrade downtime**

- Overview of BIG-IP system software upgrades - https://support.f5.com/csp/article/K84554955
- Opening a proactive service request with F5 Support - https://my.f5.com/manage/s/article/K16022
- Consider F5 Professional Services (especially for platform migration)
- K7727: License activation may be required before a software upgrade for BIG-IP - https://my.f5.com/manage/s/article/K7727
- Read Release Notes (Review release notes of any versions in-between)
- Verify Device Certificate expiration date
- Upload **QKView** to **iHealth** (or save locally)
- MD5 checksum on downloaded ISO (Security Check)
- **Create UCS backup!**



# Objective 3.03

Explain application client-server communication



Client sends SYN request to LTM Standard Virtual Server with Layer 7 functionality

LTM sends SYN-ACK TCP segment to Client

Client sends ACK packet to acknowledge receiving the SYN ACK segment from the LTM

Client-side TCP handshake is complete. The LTM waits for data packet from Client before selecting pool member

Client sends HTTP GET request

LTM chooses pool member and initiates TCP connection

LTM initiates SYN request with new ISN to pool member

Pool member sets SYN and ACK bits in the TCP header. Sends TCP segment sent to LTM

LTM acknowledges receiving SYN ACK segment from pool member

LTM sends data packet to pool member

LTM sends GET request to pool member

**Client-server communication**

The client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.

- https://en.wikipedia.org/wiki/Client–server_model
- Remember BIG-IP is a **FULL PROXY**
- SYN / SYN-ACK / ACK
- HTTP Request / HTTP Response

# Objective 3.03

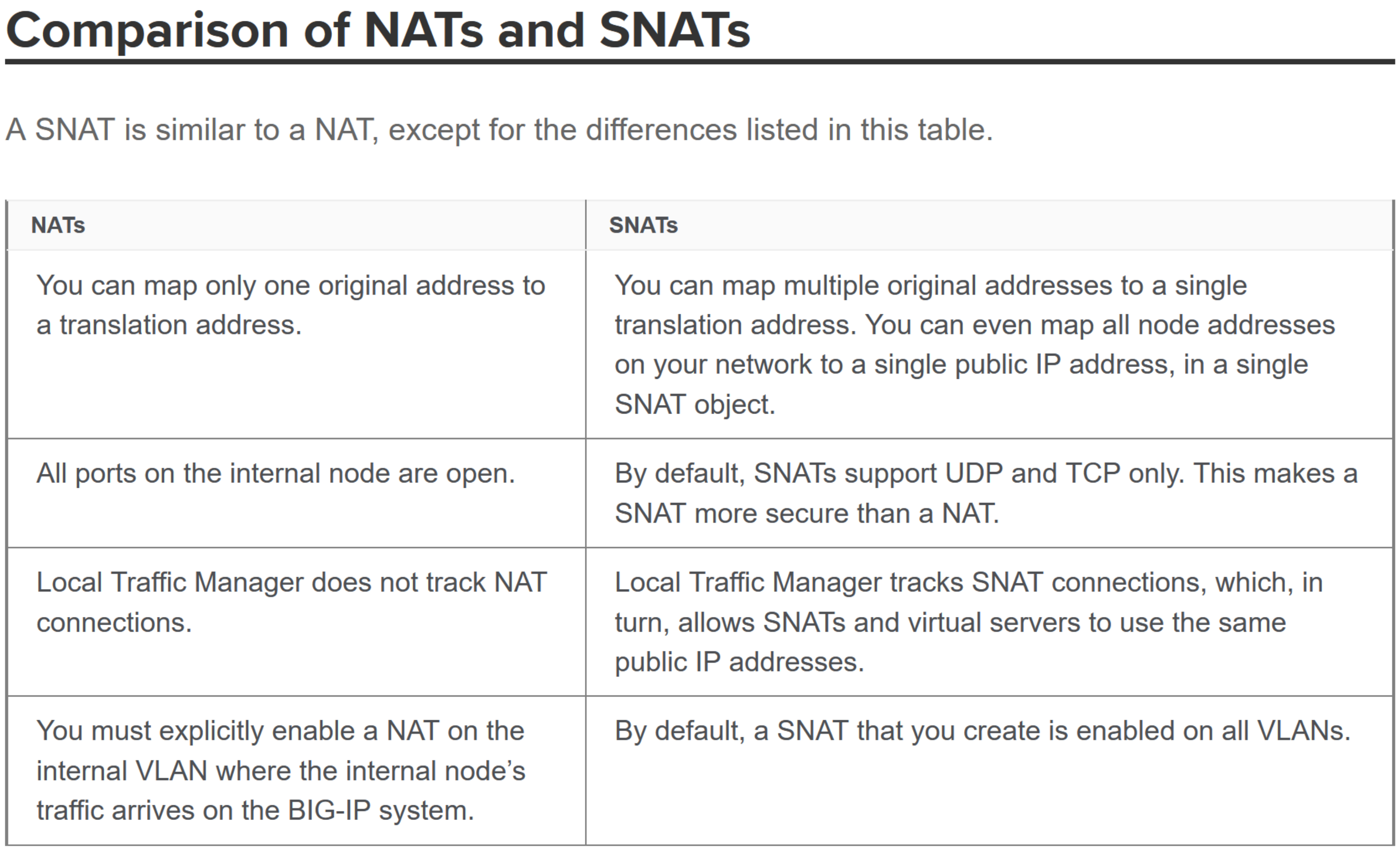
Given a scenario, interpret traffic flow

**NAT**

- One-to-one mapping
- Bi-directional “listener”
- All ports are open

**SNAT**

- One-to-many mapping
- Automap translates server-side source IP to internal self IP or floating IP
- Port exhaustion – maximum of 65,535 concurrent connections
- Use SNAT Pool



## Comparison of NATs and SNATs

A SNAT is similar to a NAT, except for the differences listed in this table.

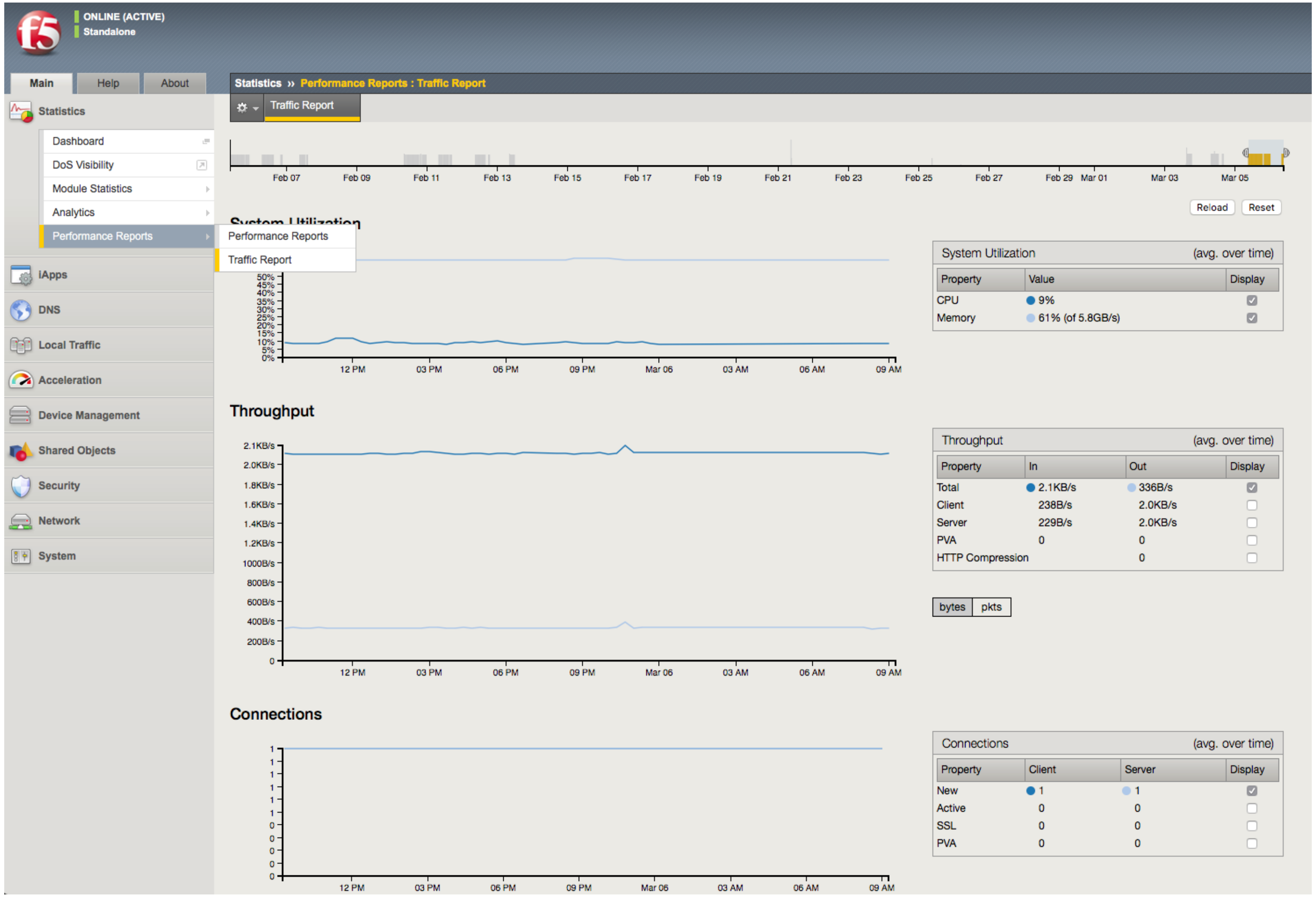
| NATs | SNATs |
|---|---|
| You can map only one original address to a translation address. | You can map multiple original addresses to a single translation address. You can even map all node addresses on your network to a single public IP address, in a single SNAT object. |
| All ports on the internal node are open. | By default, SNATs support UDP and TCP only. This makes a SNAT more secure than a NAT. |
| Local Traffic Manager does not track NAT connections. | Local Traffic Manager tracks SNAT connections, which, in turn, allows SNATs and virtual servers to use the same public IP addresses. |
| You must explicitly enable a NAT on the internal VLAN where the internal node’s traffic arrives on the BIG-IP system. | By default, a SNAT that you create is enabled on all VLANs. |

K8246: How the BIG-IP system handles SNAT port exhaustion – https://my.f5.com/manage/s/article/K8246

# Objective 3.03

Interpret traffic graphs (Interpret SNMP results)

- **Monitoring BIG-IP System Traffic with SNMP** - [https://techdocs.f5.com/en-us/bigip-15-0-0/external-monitoring-of-big-ip-systems-implementations/monitoring-big-ip-system-traffic-with-snmp.html](https://techdocs.f5.com/en-us/bigip-15-0-0/external-monitoring-of-big-ip-systems-implementations/monitoring-big-ip-system-traffic-with-snmp.html)
- Traffic Graphs



System Utilization (avg. over time)

| Property | Value | Display |
|---|---|---|
| CPU | ● 9% | ☑ |
| Memory | ● 61% (of 5.8GB/s) | ☑ |

Throughput (avg. over time)

| Property | In | Out | Display |
|---|---|---|---|
| Total | ● 2.1KB/s | ● 336B/s | ☑ |
| Client | 238B/s | 2.0KB/s | □ |
| Server | 229B/s | 2.0KB/s | □ |
| PVA | 0 | 0 | □ |
| HTTP Compression | | 0 | □ |

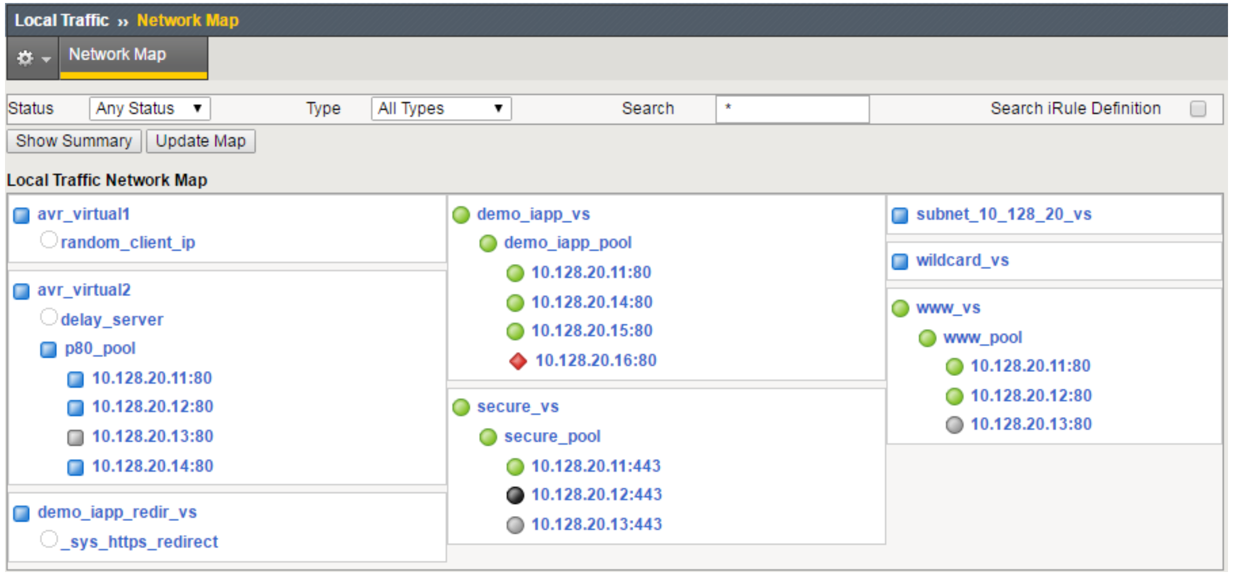
Connections (avg. over time)

| Property | Client | Server | Display |
|---|---|---|---|
| New | ● 1 | ● 1 | ☑ |
| Active | 0 | 0 | □ |
| SSL | 0 | 0 | □ |
| PVA | 0 | 0 | □ |

# Objective 3.04

## Given a scenario, interpret service status

### Compare active vs inactive ADC elements



Local Traffic » Network Map

Network Map

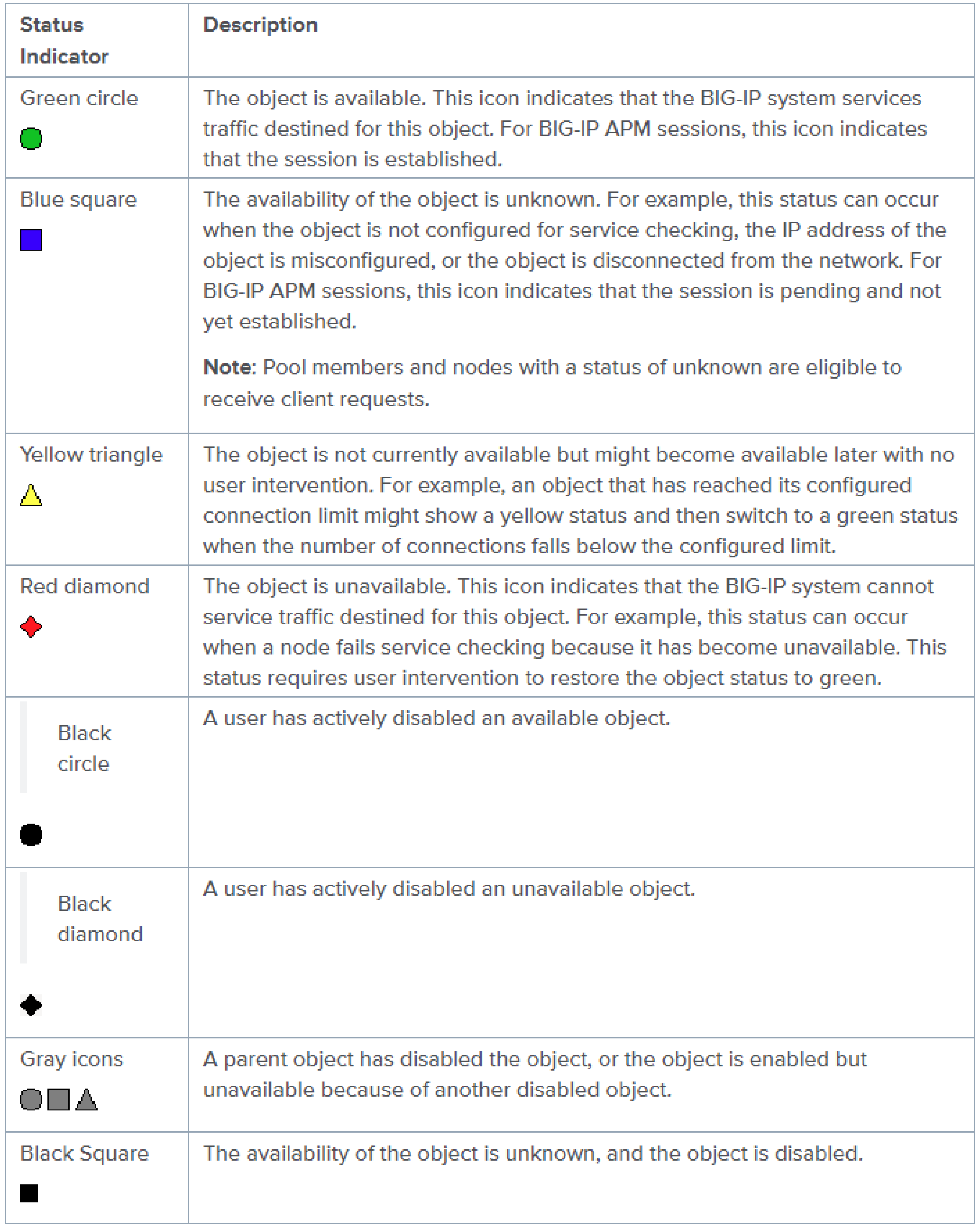
Status: Any Status ▾ Type: All Types ▾ Search: * Search iRule Definition □

Show Summary | Update Map

Local Traffic Network Map

- ■ avr_virtual1
  - ○ random_client_ip
- ■ avr_virtual2
  - ○ delay_server
  - ■ p80_pool
    - ■ 10.128.20.11:80
    - ■ 10.128.20.12:80
    - ■ 10.128.20.13:80
    - ■ 10.128.20.14:80
- ■ demo_iapp_redir_vs
  - ○ _sys_https_redirect
- ● demo_iapp_vs
  - ● demo_iapp_pool
    - ● 10.128.20.11:80
    - ● 10.128.20.14:80
    - ● 10.128.20.15:80
    - ◆ 10.128.20.16:80
- ● secure_vs
  - ● secure_pool
    - ● 10.128.20.11:443
    - ● 10.128.20.12:443
    - ● 10.128.20.13:443
- ■ subnet_10_128_20_vs
- ■ wildcard_vs
- ● www_vs
  - ● www_pool
    - ● 10.128.20.11:80
    - ● 10.128.20.12:80
    - ● 10.128.20.13:80

K12213214: Overview of colored status icons in the Configuration utility - [https://my.f5.com/manage/s/article/K12213214](https://my.f5.com/manage/s/article/K12213214)



| Status Indicator | Description |
|---|---|
| Green circle<br>● | The object is available. This icon indicates that the BIG-IP system services traffic destined for this object. For BIG-IP APM sessions, this icon indicates that the session is established. |
| Blue square<br>■ | The availability of the object is unknown. For example, this status can occur when the object is not configured for service checking, the IP address of the object is misconfigured, or the object is disconnected from the network. For BIG-IP APM sessions, this icon indicates that the session is pending and not yet established.<br>**Note:** Pool members and nodes with a status of unknown are eligible to receive client requests. |
| Yellow triangle<br>△ | The object is not currently available but might become available later with no user intervention. For example, an object that has reached its configured connection limit might show a yellow status and then switch to a green status when the number of connections falls below the configured limit. |
| Red diamond<br>◆ | The object is unavailable. This icon indicates that the BIG-IP system cannot service traffic destined for this object. For example, this status can occur when a node fails service checking because it has become unavailable. This status requires user intervention to restore the object status to green. |
| Black circle<br>● | A user has actively disabled an available object. |
| Black diamond<br>◆ | A user has actively disabled an unavailable object. |
| Gray icons<br>● ■ ▲ | A parent object has disabled the object, or the object is enabled but unavailable because of another disabled object. |
| Black Square<br>■ | The availability of the object is unknown, and the object is disabled. |

# Objective 3.04

Compare active vs inactive ADC elements

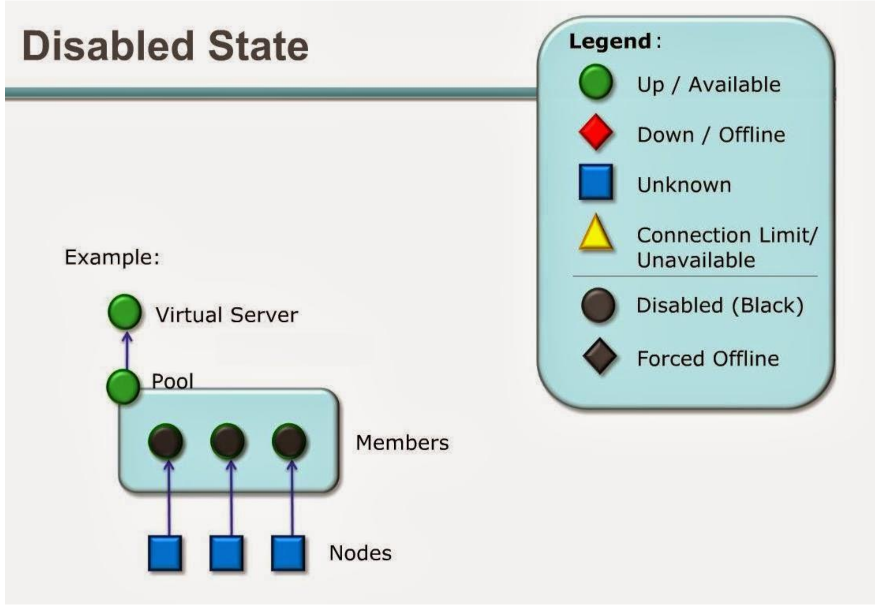
### Disabled vs Force Offline

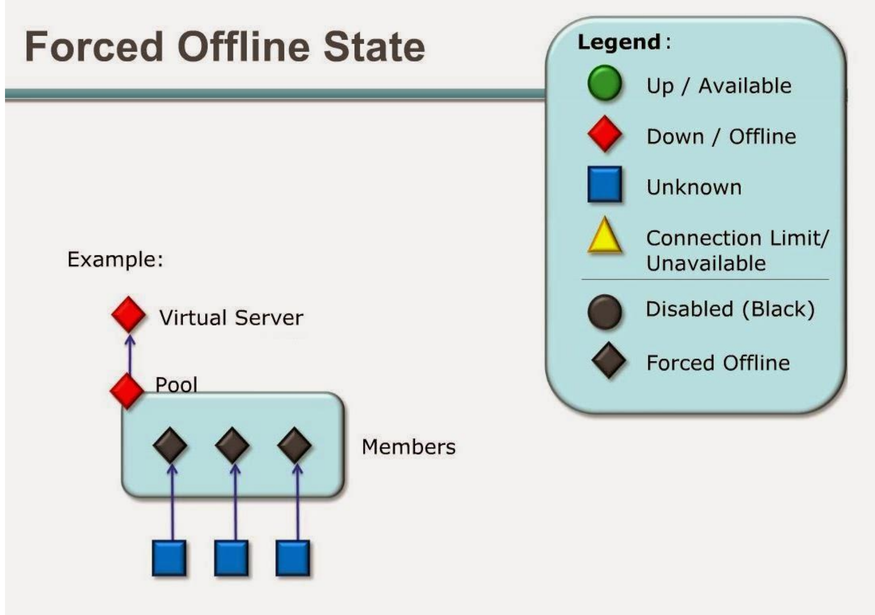
- Both will no longer accept new connections
- Both still accepts traffic from an active connections (ssh and ftp)
- Disabled still accepts traffic from existing persistence records
- Force Offline drops traffic even from existing persistence records

### Manual Resume

- When BIG-IP marks a server offline
- Must be manually enabled

**Enabling and Disabling Local Traffic Objects –** [https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0/enabling-and-disabling-local-traffic-objects.html](https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0/enabling-and-disabling-local-traffic-objects.html)

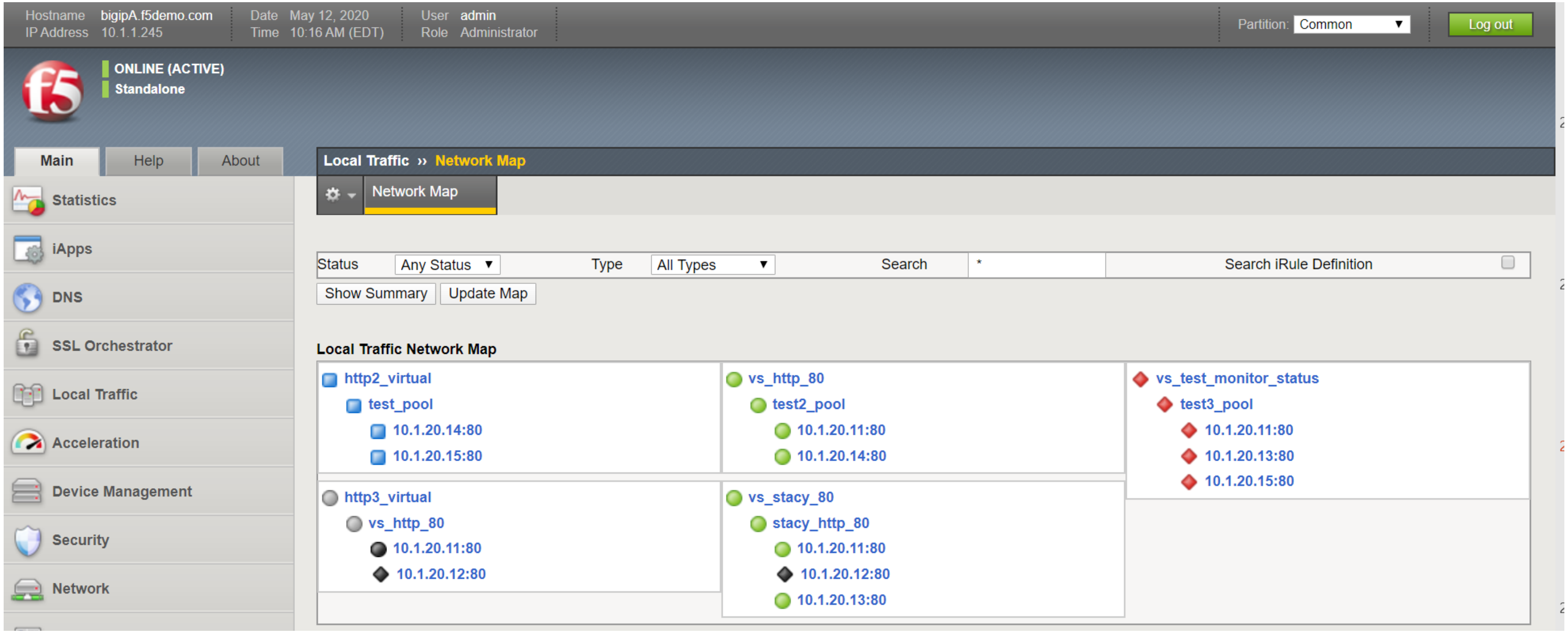




# Objective 3.04

Given a scenario, interpret service status

## Status icons in Network Map



Hostname bigipA.f5demo.com
IP Address 10.1.1.245

Date May 12, 2020
Time 10:16 AM (EDT)

User admin
Role Administrator

Partition: Common

ONLINE (ACTIVE)
Standalone

Local Traffic ›› Network Map

Status: Any Status | Type: All Types | Search: * | Search iRule Definition ☐

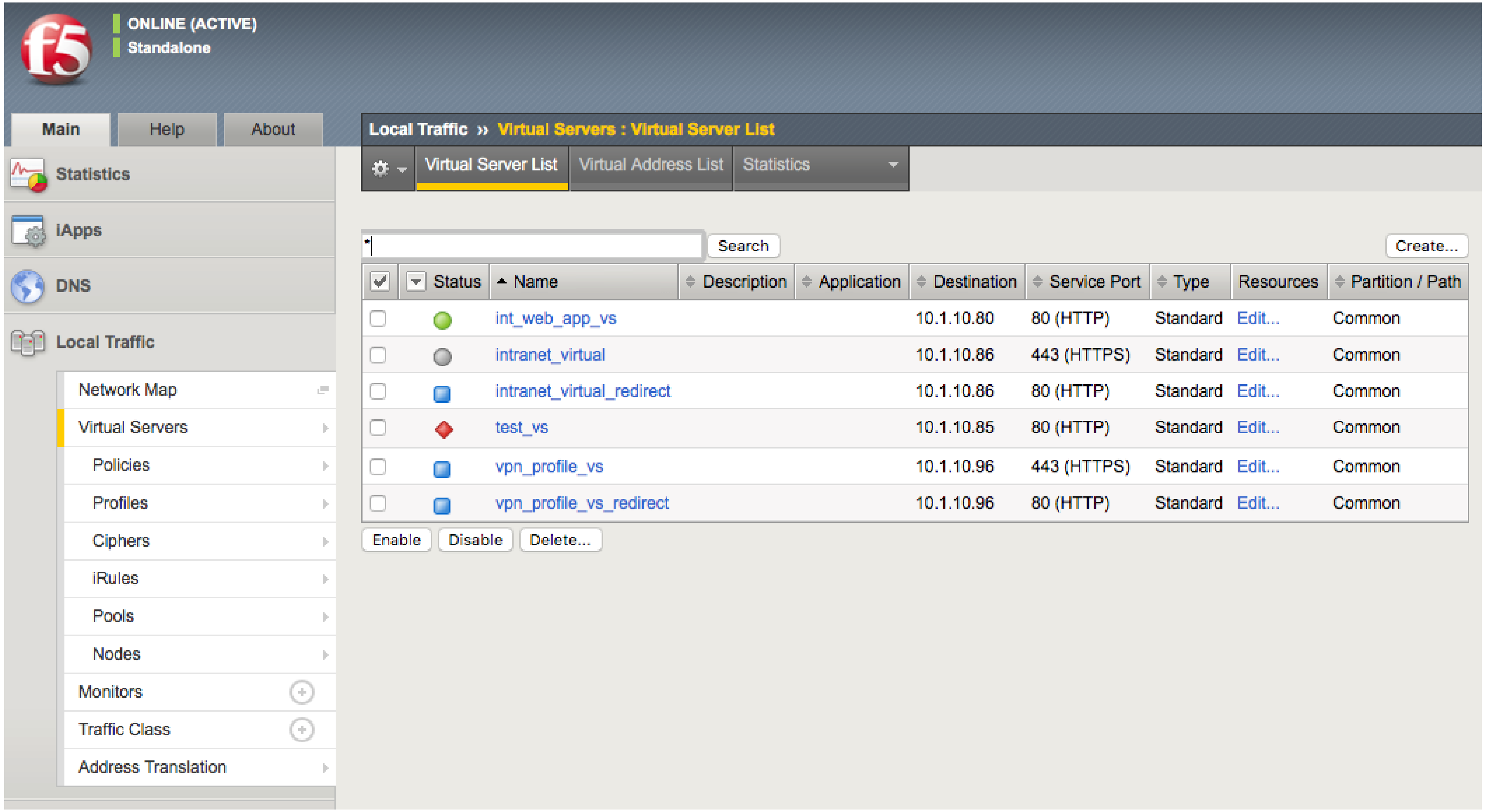
**Local Traffic Network Map**

- 🟦 http2_virtual
  - 🟦 test_pool
    - 🟦 10.1.20.14:80
    - 🟦 10.1.20.15:80
- ⚪ http3_virtual
  - ⚪ vs_http_80
    - ⚫ 10.1.20.11:80
    - ◆ 10.1.20.12:80
- 🟢 vs_http_80
  - 🟢 test2_pool
    - 🟢 10.1.20.11:80
    - 🟢 10.1.20.14:80
- 🟢 vs_stacy_80
  - 🟢 stacy_http_80
    - 🟢 10.1.20.11:80
    - ◆ 10.1.20.12:80
    - 🟢 10.1.20.13:80
- ♦ vs_test_monitor_status
  - ♦ test3_pool
    - ♦ 10.1.20.11:80
    - ♦ 10.1.20.13:80
    - ♦ 10.1.20.15:80

# Objective 3.04

Given a scenario, interpret service status

### Status icons for configuration objects in the GUI

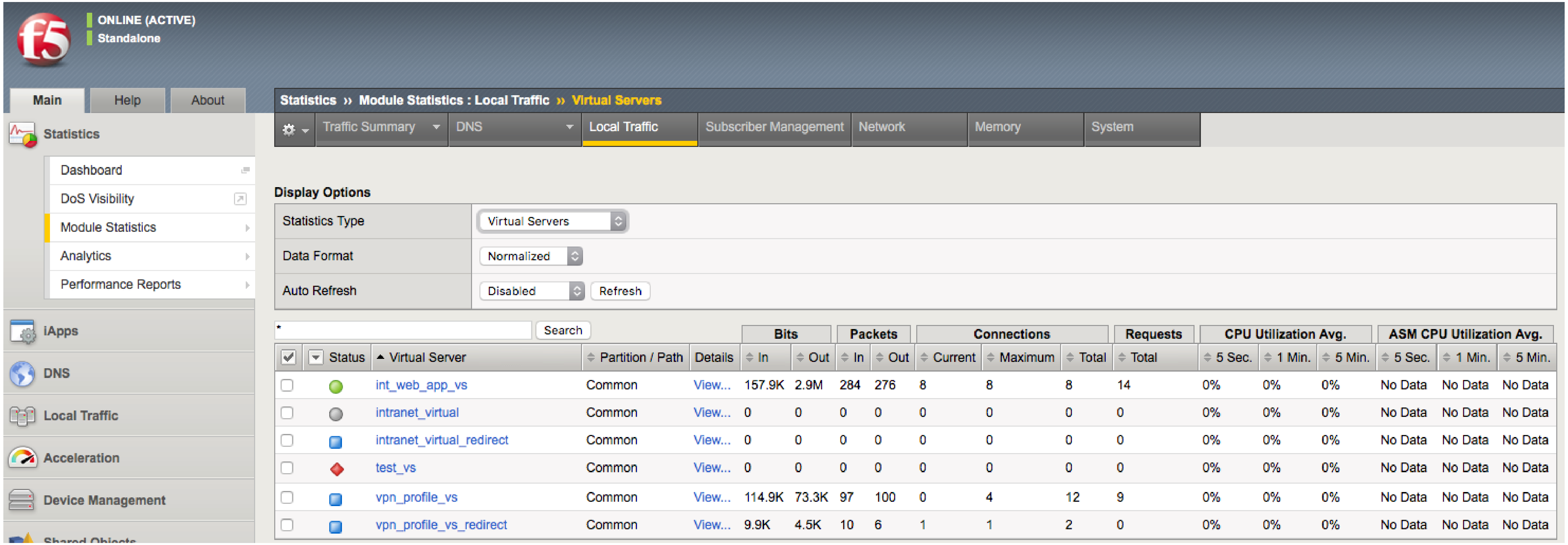


| ☑ | Status | Name | Description | Application | Destination | Service Port | Type | Resources | Partition / Path |
|---|---|---|---|---|---|---|---|---|---|
| □ | 🟢 | int_web_app_vs | | | 10.1.10.80 | 80 (HTTP) | Standard | Edit... | Common |
| □ | ● | intranet_virtual | | | 10.1.10.86 | 443 (HTTPS) | Standard | Edit... | Common |
| □ | 🟦 | intranet_virtual_redirect | | | 10.1.10.86 | 80 (HTTP) | Standard | Edit... | Common |
| □ | ♦ | test_vs | | | 10.1.10.85 | 80 (HTTP) | Standard | Edit... | Common |
| □ | 🟦 | vpn_profile_vs | | | 10.1.10.96 | 443 (HTTPS) | Standard | Edit... | Common |
| □ | 🟦 | vpn_profile_vs_redirect | | | 10.1.10.96 | 80 (HTTP) | Standard | Edit... | Common |

# Objective 3.04

Given a scenario, interpret service status

**Traffic statistics indicating which objects are or are not actively receiving traffic.**



ONLINE (ACTIVE)
Standalone

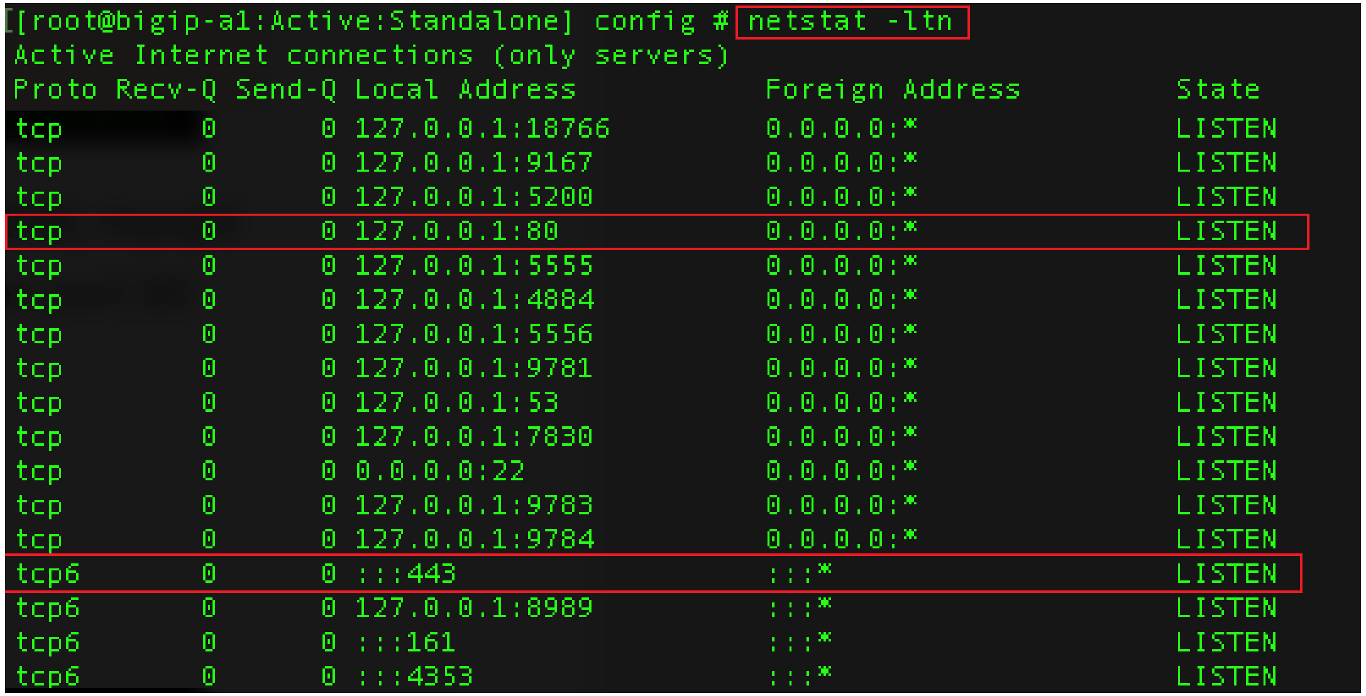
**Display Options**

| | |
|---|---|
| Statistics Type | Virtual Servers |
| Data Format | Normalized |
| Auto Refresh | Disabled |

| | | | | | Bits | | Packets | | Connections | | | Requests | CPU Utilization Avg. | | | ASM CPU Utilization Avg. | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Status | Virtual Server | Partition / Path | Details | In | Out | In | Out | Current | Maximum | Total | Total | 5 Sec. | 1 Min. | 5 Min. | 5 Sec. | 1 Min. | 5 Min. |
| □ | 🟢 | int_web_app_vs | Common | View... | 157.9K | 2.9M | 284 | 276 | 8 | 8 | 8 | 14 | 0% | 0% | 0% | No Data | No Data | No Data |
| □ | ● | intranet_virtual | Common | View... | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0% | 0% | No Data | No Data | No Data |
| □ | 🟦 | intranet_virtual_redirect | Common | View... | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0% | 0% | No Data | No Data | No Data |
| □ | ♦ | test_vs | Common | View... | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0% | 0% | No Data | No Data | No Data |
| □ | 🟦 | vpn_profile_vs | Common | View... | 114.9K | 73.3K | 97 | 100 | 0 | 4 | 12 | 9 | 0% | 0% | 0% | No Data | No Data | No Data |
| □ | 🟦 | vpn_profile_vs_redirect | Common | View... | 9.9K | 4.5K | 10 | 6 | 1 | 1 | 2 | 0 | 0% | 0% | 0% | No Data | No Data | No Data |

# Objective 3.04

Infer services for given netstat output



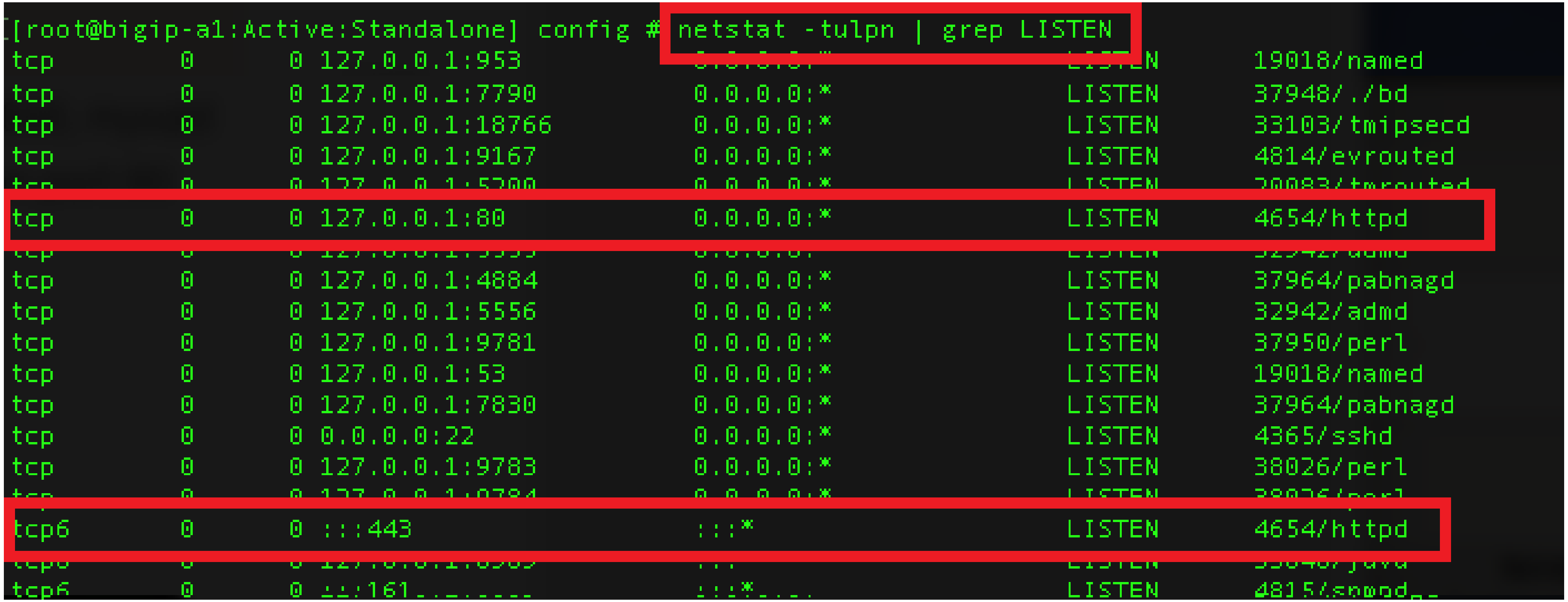
```
[root@bigip-a1:Active:Standalone] config # netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address              Foreign Address            State
tcp        0      0 127.0.0.1:18766            0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:9167             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:5200             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:80               0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:5555             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:4884             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:5556             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:9781             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:53               0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:7830             0.0.0.0:*                  LISTEN
tcp        0      0 0.0.0.0:22                 0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:9783             0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:9784             0.0.0.0:*                  LISTEN
tcp6       0      0 :::443                     :::*                       LISTEN
tcp6       0      0 127.0.0.1:8989             :::*                       LISTEN
tcp6       0      0 :::161                     :::*                       LISTEN
tcp6       0      0 :::4353                    :::*                       LISTEN
```

List of TCP and UDP port numbers –
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

# Objective 3.04

Given a scenario, interpret service status

**netstat -tulpn | grep LISTEN**

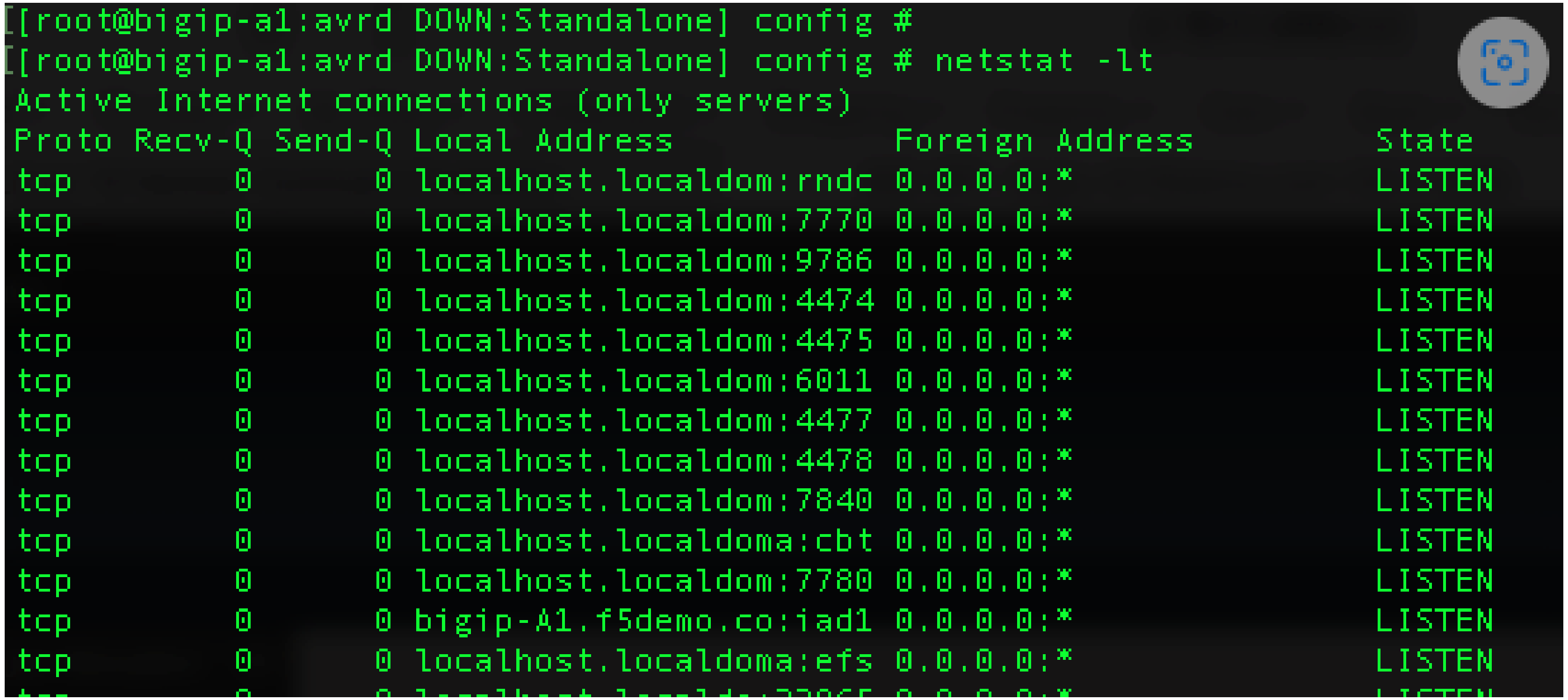


```
[root@bigip-a1:Active:Standalone] config # netstat -tulpn | grep LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      19018/named
tcp        0      0 127.0.0.1:7790          0.0.0.0:*               LISTEN      37948/./bd
tcp        0      0 127.0.0.1:18766         0.0.0.0:*               LISTEN      33103/tmipsecd
tcp        0      0 127.0.0.1:9167          0.0.0.0:*               LISTEN      4814/evrouted
tcp        0      0 127.0.0.1:5300          0.0.0.0:*               LISTEN      20083/tmrouted
tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN      4654/httpd
tcp        0      0 127.0.0.1:5555          0.0.0.0:*               LISTEN      32942/admd
tcp        0      0 127.0.0.1:4884          0.0.0.0:*               LISTEN      37964/pabnagd
tcp        0      0 127.0.0.1:5556          0.0.0.0:*               LISTEN      32942/admd
tcp        0      0 127.0.0.1:9781          0.0.0.0:*               LISTEN      37950/perl
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      19018/named
tcp        0      0 127.0.0.1:7830          0.0.0.0:*               LISTEN      37964/pabnagd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4365/sshd
tcp        0      0 127.0.0.1:9783          0.0.0.0:*               LISTEN      38026/perl
tcp        0      0 127.0.0.1:9784          0.0.0.0:*               LISTEN      38026/perl
tcp6       0      0 :::443                  :::*                    LISTEN      4654/httpd
tcp6       0      0 127.0.0.1:[illegible]   :::*                    LISTEN      [illegible]/java
tcp6       0      0 :::161                  :::*                    LISTEN      4815/snmpd
```

# Objective 3.04

Determine whether a service is listening on a given port based on netstat output

## Netstat Output



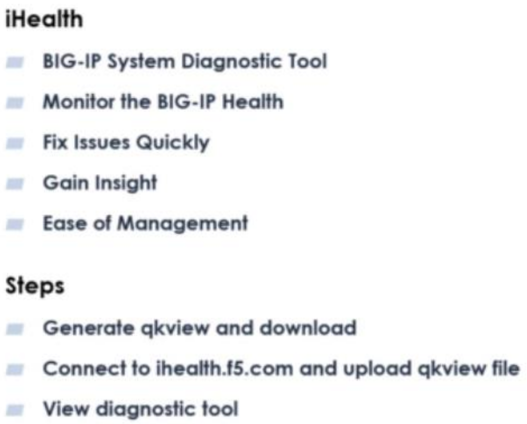
```
[[root@bigip-a1:avrd DOWN:Standalone] config #
[[root@bigip-a1:avrd DOWN:Standalone] config # netstat -lt
 Active Internet connections (only servers)
 Proto Recv-Q Send-Q Local Address               Foreign Address         State
 tcp        0      0 localhost.localdom:rndc 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:7770 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:9786 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:4474 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:4475 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:6011 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:4477 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:4478 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:7840 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdoma:cbt 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdom:7780 0.0.0.0:*               LISTEN
 tcp        0      0 bigip-A1.f5demo.co:iad1 0.0.0.0:*               LISTEN
 tcp        0      0 localhost.localdoma:efs 0.0.0.0:*               LISTEN
```

https://www.thegeekstuff.com/2010/03/netstat-command-examples/

# Objective 3.05

## Generate a Qkview and upload to iHealth

- https://ihealth.f5.com/qkview-analyzer/
  - K12878: Generating diagnostic data using the qkview utility - https://support.f5.com/csp/article/K12878
  - **QKview** - The qkview utility is an executable program that generates machine-readable (XML) diagnostic data and combines the data into a single compressed Tape ARchive (TAR) format file. You can upload this file, called a QKView file, to F5 iHealth , or give it to F5 Support to help them troubleshoot any issues.

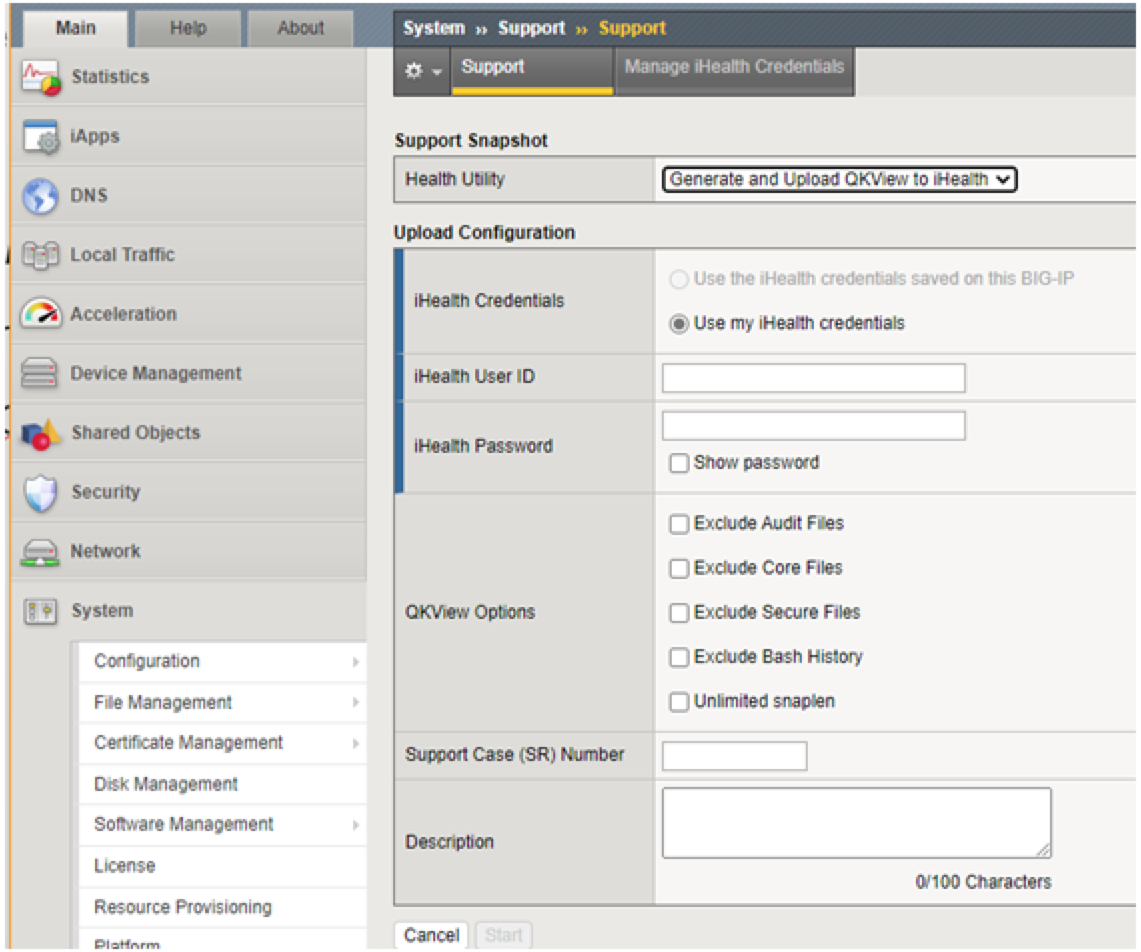


**iHealth**

- BIG-IP System Diagnostic Tool
- Monitor the BIG-IP Health
- Fix Issues Quickly
- Gain Insight
- Ease of Management

**Steps**

- Generate qkview and download
- Connect to ihealth.f5.com and upload qkview file
- View diagnostic tool



**Support Snapshot**

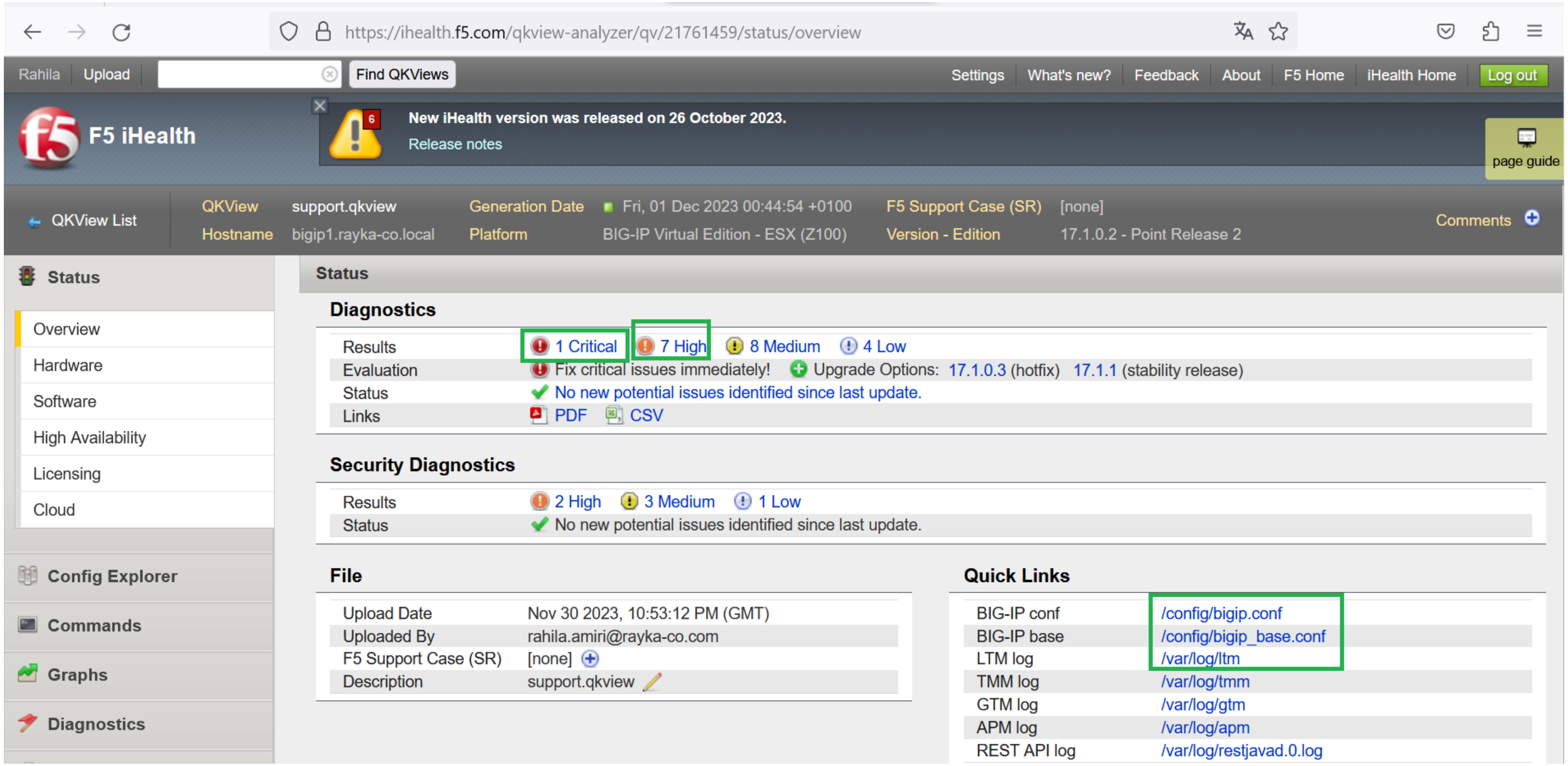
| | |
|---|---|
| Health Utility | Generate and Upload QKView to iHealth |

**Upload Configuration**

| | |
|---|---|
| iHealth Credentials | ○ Use the iHealth credentials saved on this BIG-IP<br>● Use my iHealth credentials |
| iHealth User ID | |
| iHealth Password | □ Show password |
| QKView Options | □ Exclude Audit Files<br>□ Exclude Core Files<br>□ Exclude Secure Files<br>□ Exclude Bash History<br>□ Unlimited snaplen |
| Support Case (SR) Number | |
| Description | 0/100 Characters |

# Objective 3.05

Generate a Qkview and upload to iHealth



https://ihealth.f5.com/qkview-analyzer/qv/21761459/status/overview

Rahila | Upload | Find QKViews | Settings | What's new? | Feedback | About | F5 Home | iHealth Home | Log out

F5 iHealth

New iHealth version was released on 26 October 2023.
Release notes

page guide

QKView List

| | | | | | |
|---|---|---|---|---|---|
| QKView | support.qkview | Generation Date | Fri, 01 Dec 2023 00:44:54 +0100 | F5 Support Case (SR) | [none] |
| Hostname | bigip1.rayka-co.local | Platform | BIG-IP Virtual Edition - ESX (Z100) | Version - Edition | 17.1.0.2 - Point Release 2 |

Comments

Status

**Diagnostics**

| | |
|---|---|
| Results | 1 Critical 7 High 8 Medium 4 Low |
| Evaluation | Fix critical issues immediately! Upgrade Options: 17.1.0.3 (hotfix) 17.1.1 (stability release) |
| Status | ✓ No new potential issues identified since last update. |
| Links | PDF CSV |

**Security Diagnostics**

| | |
|---|---|
| Results | 2 High 3 Medium 1 Low |
| Status | ✓ No new potential issues identified since last update. |

**File**

| | |
|---|---|
| Upload Date | Nov 30 2023, 10:53:12 PM (GMT) |
| Uploaded By | rahila.amiri@rayka-co.com |
| F5 Support Case (SR) | [none] |
| Description | support.qkview |

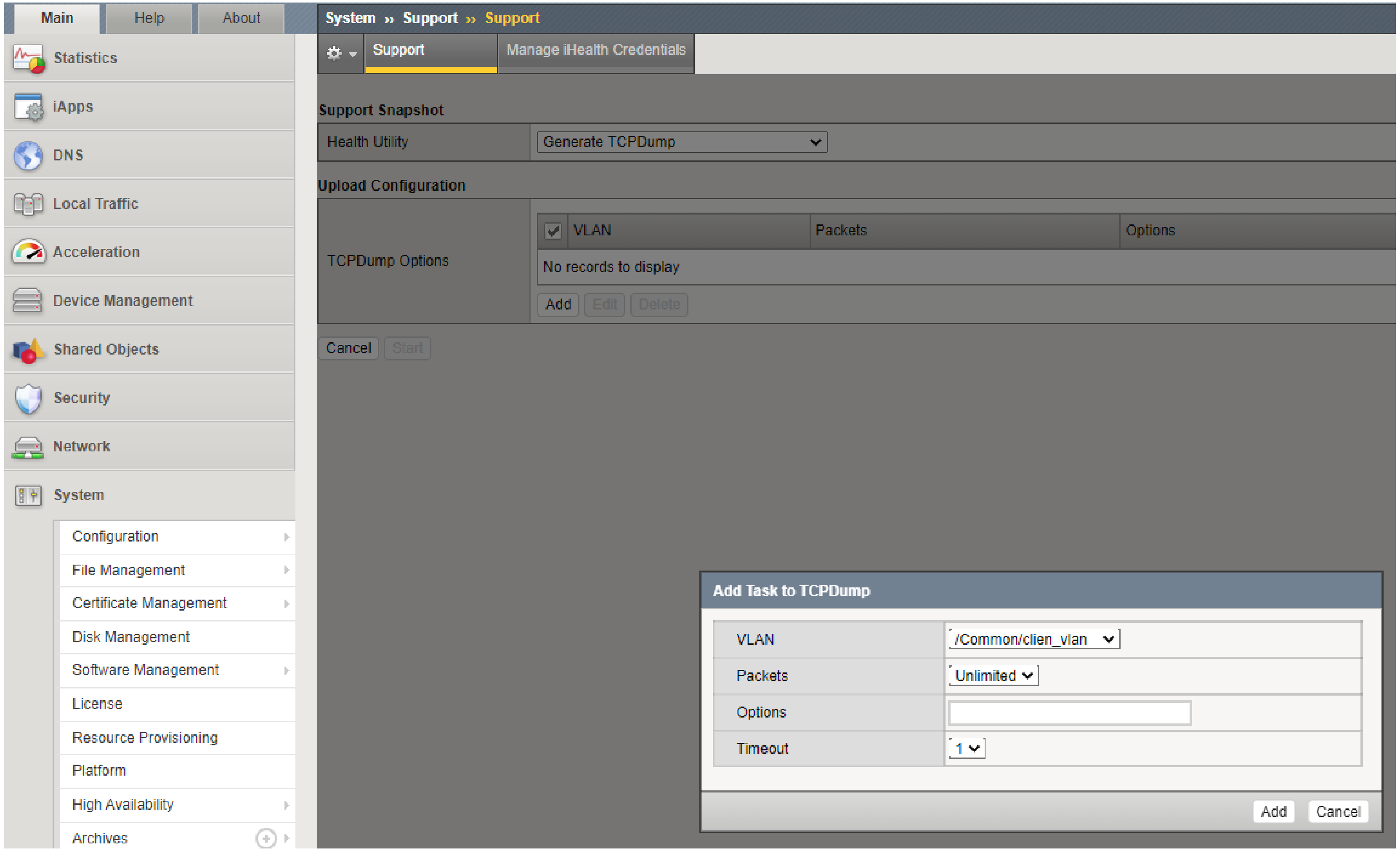
**Quick Links**

| | |
|---|---|
| BIG-IP conf | /config/bigip.conf |
| BIG-IP base | /config/bigip_base.conf |
| LTM log | /var/log/ltm |
| TMM log | /var/log/tmm |
| GTM log | /var/log/gtm |
| APM log | /var/log/apm |
| REST API log | /var/log/restjavad.0.log |

# Objective 3.05

Given a scenario, interpret system health

## TCPDump from TMUI



**Support Snapshot**

| | |
|---|---|
| Health Utility | Generate TCPDump |

**Upload Configuration**

TCPDump Options

| ☑ VLAN | Packets | Options |
|---|---|---|
| No records to display | | |

**Add Task to TCPDump**

| | |
|---|---|
| VLAN | /Common/clien_vlan |
| Packets | Unlimited |
| Options | |
| Timeout | 1 |

# Objective 3.05

## Review Logs

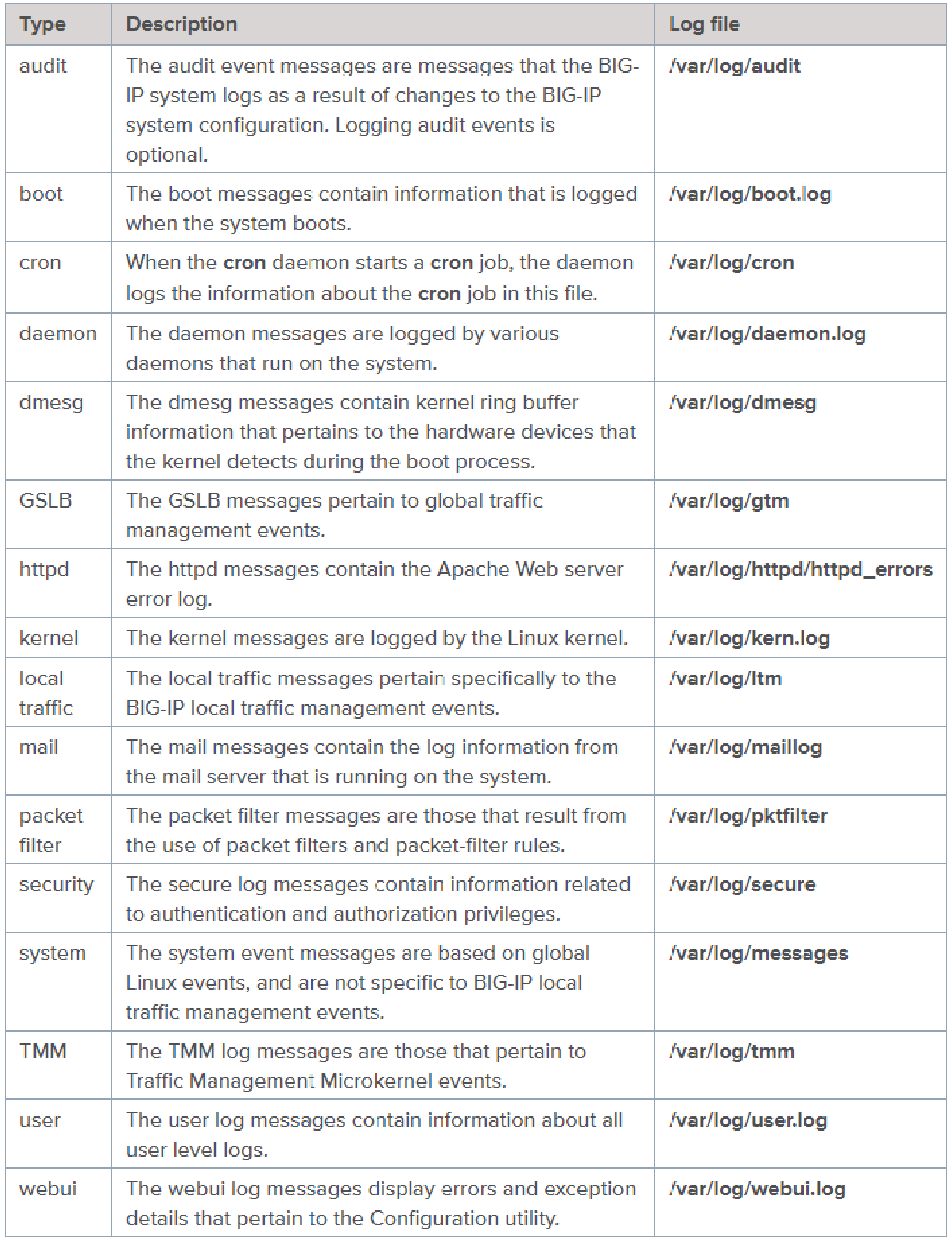
### Local logging

- By default, the BIG-IP system logs events locally and stores messages in the **/var/log** directory. For BIG-IP events, the system routes messages from the **errdefs** subsystem through **syslog-ng** to the local log files. For non-BIG-IP events, the system routes messages directly through **syslog-ng** to the local log files. In addition, you can configure the system to use the high-speed logging mechanism (HSL) to store the logs in either the **syslog** or the MySQL database.

### Remote logging

- You can configure the system to use the HSL mechanism to log messages to a pool of remote log servers. If the BIG-IP system processes a high volume of traffic or generates an excessive amount of log files, F5 recommends that you configure HSL remote logging.

**K16197: Reviewing BIG-IP log files –**
[https://support.f5.com/csp/article/K16197](https://support.f5.com/csp/article/K16197)

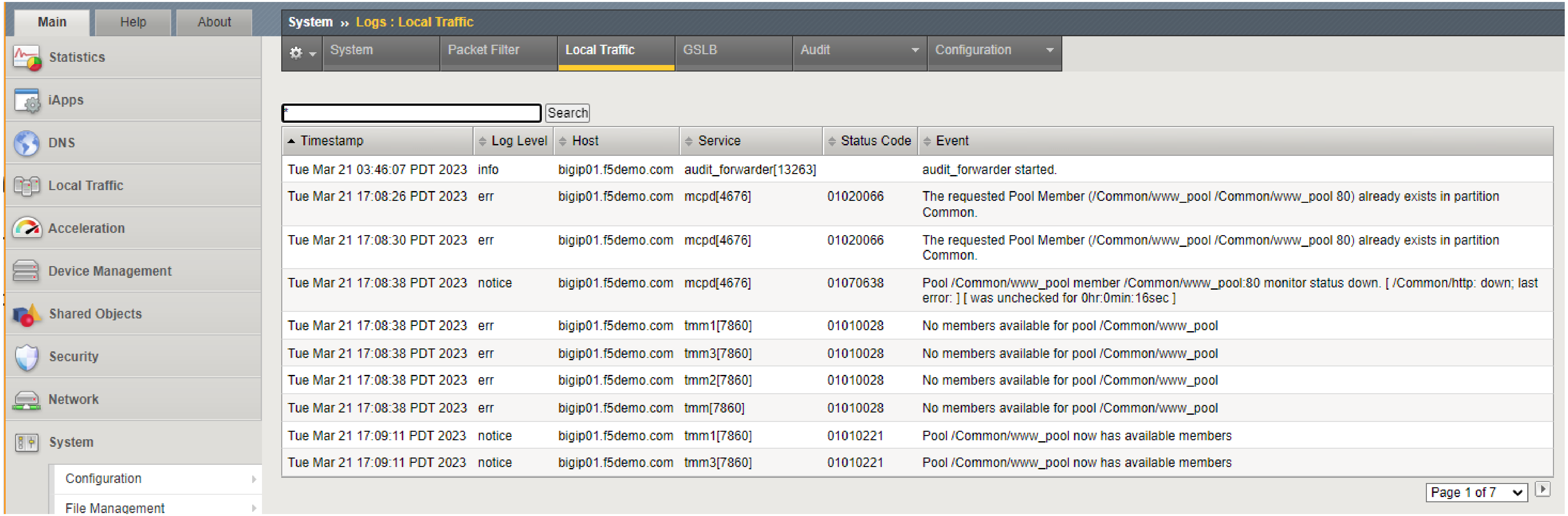


| Type | Description | Log file |
|---|---|---|
| audit | The audit event messages are messages that the BIG-IP system logs as a result of changes to the BIG-IP system configuration. Logging audit events is optional. | **/var/log/audit** |
| boot | The boot messages contain information that is logged when the system boots. | **/var/log/boot.log** |
| cron | When the **cron** daemon starts a **cron** job, the daemon logs the information about the **cron** job in this file. | **/var/log/cron** |
| daemon | The daemon messages are logged by various daemons that run on the system. | **/var/log/daemon.log** |
| dmesg | The dmesg messages contain kernel ring buffer information that pertains to the hardware devices that the kernel detects during the boot process. | **/var/log/dmesg** |
| GSLB | The GSLB messages pertain to global traffic management events. | **/var/log/gtm** |
| httpd | The httpd messages contain the Apache Web server error log. | **/var/log/httpd/httpd_errors** |
| kernel | The kernel messages are logged by the Linux kernel. | **/var/log/kern.log** |
| local traffic | The local traffic messages pertain specifically to the BIG-IP local traffic management events. | **/var/log/ltm** |
| mail | The mail messages contain the log information from the mail server that is running on the system. | **/var/log/maillog** |
| packet filter | The packet filter messages are those that result from the use of packet filters and packet-filter rules. | **/var/log/pktfilter** |
| security | The secure log messages contain information related to authentication and authorization privileges. | **/var/log/secure** |
| system | The system event messages are based on global Linux events, and are not specific to BIG-IP local traffic management events. | **/var/log/messages** |
| TMM | The TMM log messages are those that pertain to Traffic Management Microkernel events. | **/var/log/tmm** |
| user | The user log messages contain information about all user level logs. | **/var/log/user.log** |
| webui | The webui log messages display errors and exception details that pertain to the Configuration utility. | **/var/log/webui.log** |

# Objective 3.05

Given a scenario, interpret system health

## Local Traffic Log



| Timestamp | Log Level | Host | Service | Status Code | Event |
|---|---|---|---|---|---|
| Tue Mar 21 03:46:07 PDT 2023 | info | bigip01.f5demo.com | audit_forwarder[13263] | | audit_forwarder started. |
| Tue Mar 21 17:08:26 PDT 2023 | err | bigip01.f5demo.com | mcpd[4676] | 01020066 | The requested Pool Member (/Common/www_pool /Common/www_pool 80) already exists in partition Common. |
| Tue Mar 21 17:08:30 PDT 2023 | err | bigip01.f5demo.com | mcpd[4676] | 01020066 | The requested Pool Member (/Common/www_pool /Common/www_pool 80) already exists in partition Common. |
| Tue Mar 21 17:08:38 PDT 2023 | notice | bigip01.f5demo.com | mcpd[4676] | 01070638 | Pool /Common/www_pool member /Common/www_pool:80 monitor status down. [ /Common/http: down; last error: ] [ was unchecked for 0hr:0min:16sec ] |
| Tue Mar 21 17:08:38 PDT 2023 | err | bigip01.f5demo.com | tmm1[7860] | 01010028 | No members available for pool /Common/www_pool |
| Tue Mar 21 17:08:38 PDT 2023 | err | bigip01.f5demo.com | tmm3[7860] | 01010028 | No members available for pool /Common/www_pool |
| Tue Mar 21 17:08:38 PDT 2023 | err | bigip01.f5demo.com | tmm2[7860] | 01010028 | No members available for pool /Common/www_pool |
| Tue Mar 21 17:08:38 PDT 2023 | err | bigip01.f5demo.com | tmm[7860] | 01010028 | No members available for pool /Common/www_pool |
| Tue Mar 21 17:09:11 PDT 2023 | notice | bigip01.f5demo.com | tmm1[7860] | 01010221 | Pool /Common/www_pool now has available members |
| Tue Mar 21 17:09:11 PDT 2023 | notice | bigip01.f5demo.com | tmm3[7860] | 01010221 | Pool /Common/www_pool now has available members |

**Using the Configuration utility to review log files**

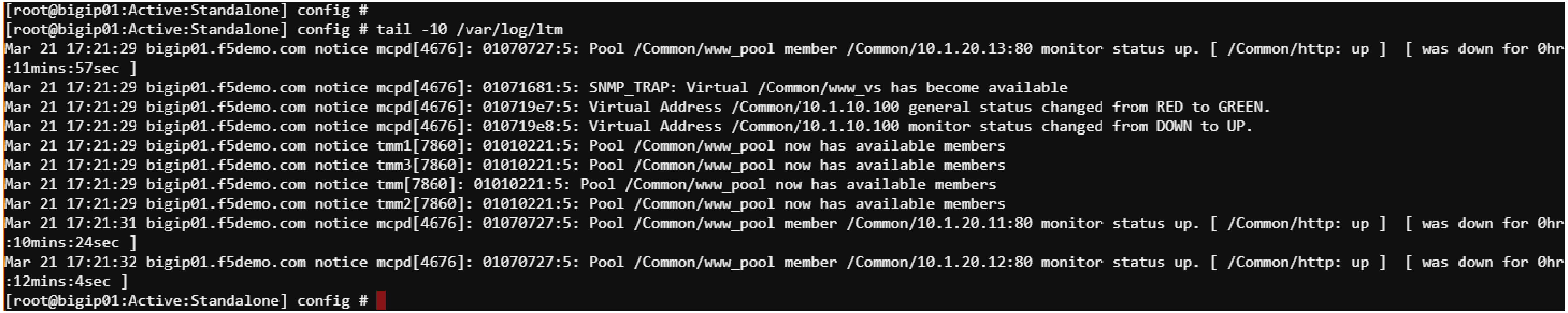
The most commonly used log files (for example, System, Local Traffic, Audit) are displayed in the Configuration utility. To review log files using the Configuration utility, perform the following steps:

1. Log in to the Configuration utility.
2. Navigate to **System > Logs.**
3. Click the tab that corresponds to the type of logging category you want to review.
4. Use the Search field to search for event strings or use the drop-down menu to page through the available logs.

# Objective 3.05

## Given a scenario, interpret system health

### Local Traffic Log



```
[root@bigip01:Active:Standalone] config #
[root@bigip01:Active:Standalone] config # tail -10 /var/log/ltm
Mar 21 17:21:29 bigip01.f5demo.com notice mcpd[4676]: 01070727:5: Pool /Common/www_pool member /Common/10.1.20.13:80 monitor status up. [ /Common/http: up ]  [ was down for 0hr
:11mins:57sec ]
Mar 21 17:21:29 bigip01.f5demo.com notice mcpd[4676]: 01071681:5: SNMP_TRAP: Virtual /Common/www_vs has become available
Mar 21 17:21:29 bigip01.f5demo.com notice mcpd[4676]: 010719e7:5: Virtual Address /Common/10.1.10.100 general status changed from RED to GREEN.
Mar 21 17:21:29 bigip01.f5demo.com notice mcpd[4676]: 010719e8:5: Virtual Address /Common/10.1.10.100 monitor status changed from DOWN to UP.
Mar 21 17:21:29 bigip01.f5demo.com notice tmm1[7860]: 01010221:5: Pool /Common/www_pool now has available members
Mar 21 17:21:29 bigip01.f5demo.com notice tmm3[7860]: 01010221:5: Pool /Common/www_pool now has available members
Mar 21 17:21:29 bigip01.f5demo.com notice tmm[7860]: 01010221:5: Pool /Common/www_pool now has available members
Mar 21 17:21:29 bigip01.f5demo.com notice tmm2[7860]: 01010221:5: Pool /Common/www_pool now has available members
Mar 21 17:21:31 bigip01.f5demo.com notice mcpd[4676]: 01070727:5: Pool /Common/www_pool member /Common/10.1.20.11:80 monitor status up. [ /Common/http: up ]  [ was down for 0hr
:10mins:24sec ]
Mar 21 17:21:32 bigip01.f5demo.com notice mcpd[4676]: 01070727:5: Pool /Common/www_pool member /Common/10.1.20.12:80 monitor status up. [ /Common/http: up ]  [ was down for 0hr
:12mins:4sec ]
[root@bigip01:Active:Standalone] config #
```

**Useful TMSH Log Commands:**
tmsh show /sys log ltm
tmsh show /sys log <log> range <date range>
tmsh show /sys log <log> range <date range> lines <maximum line count>

**Using bash to review log files:**
cd /var/log
cat ltm
more ltm

**Reviewing Archived log files:**
cd /var/log
zcat ltm.2.gz

**Using code expansion to view log files:**
cd /var/log
cat <log> |bigcodes |less

**Expanded Message Code Example:**
Mar 5 08:34:00 bigip_1 err mcpd[7430]: 01070366 (Product=BIGIP Subset=MCPD) :3: Bad password (abc123): BAD PASSWORD: it is WAY too short

# Objective 3.05

Ensure efficacy of maintenance tasks (alert endpoints, verify backups)

There are many maintenance tasks required to manage any system successfully. The BIG-IP TMOS operations guide is a great place to start understanding the basic tasks and how often they need to be done as well as links to the guides on how to do the tasks successfully.

**K34421741: Quick start guides | BIG-IP TMOS operations guide –** https://support.f5.com/csp/article/K34421741

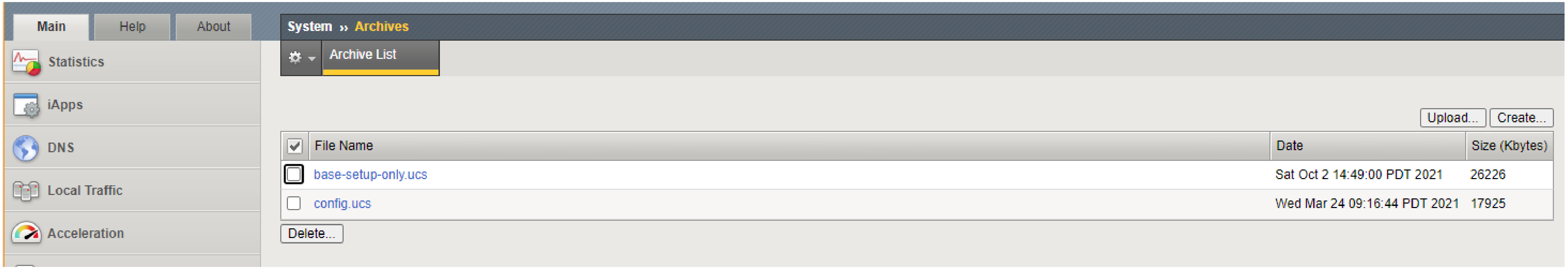
**Examples of activities include:**

- One-time tasks
- Daily tasks
- Weekly tasks
- Twice-monthly tasks
- Monthly tasks
- Quarterly tasks
- Twice-yearly tasks
- Yearly tasks
- As-needed tasks
- Maintenance Checklist

# Objective 3.05

Ensure efficacy of maintenance tasks (alert endpoints, verify backups)

**Archive list**



| ☑ | File Name | Date | Size (Kbytes) |
|---|---|---|---|
| □ | base-setup-only.ucs | Sat Oct 2 14:49:00 PDT 2021 | 26226 |
| □ | config.ucs | Wed Mar 24 09:16:44 PDT 2021 | 17925 |

K13132: Backing up and restoring BIG-IP configuration files with a UCS archive – https://my.f5.com/manage/s/article/K13132

K4422: Viewing and modifying the files that are configured for inclusion in a UCS archive – https://my.f5.com/manage/s/article/K4422

# Objective 3.05

Ensure efficacy of maintenance tasks (alert endpoints, verify backups)

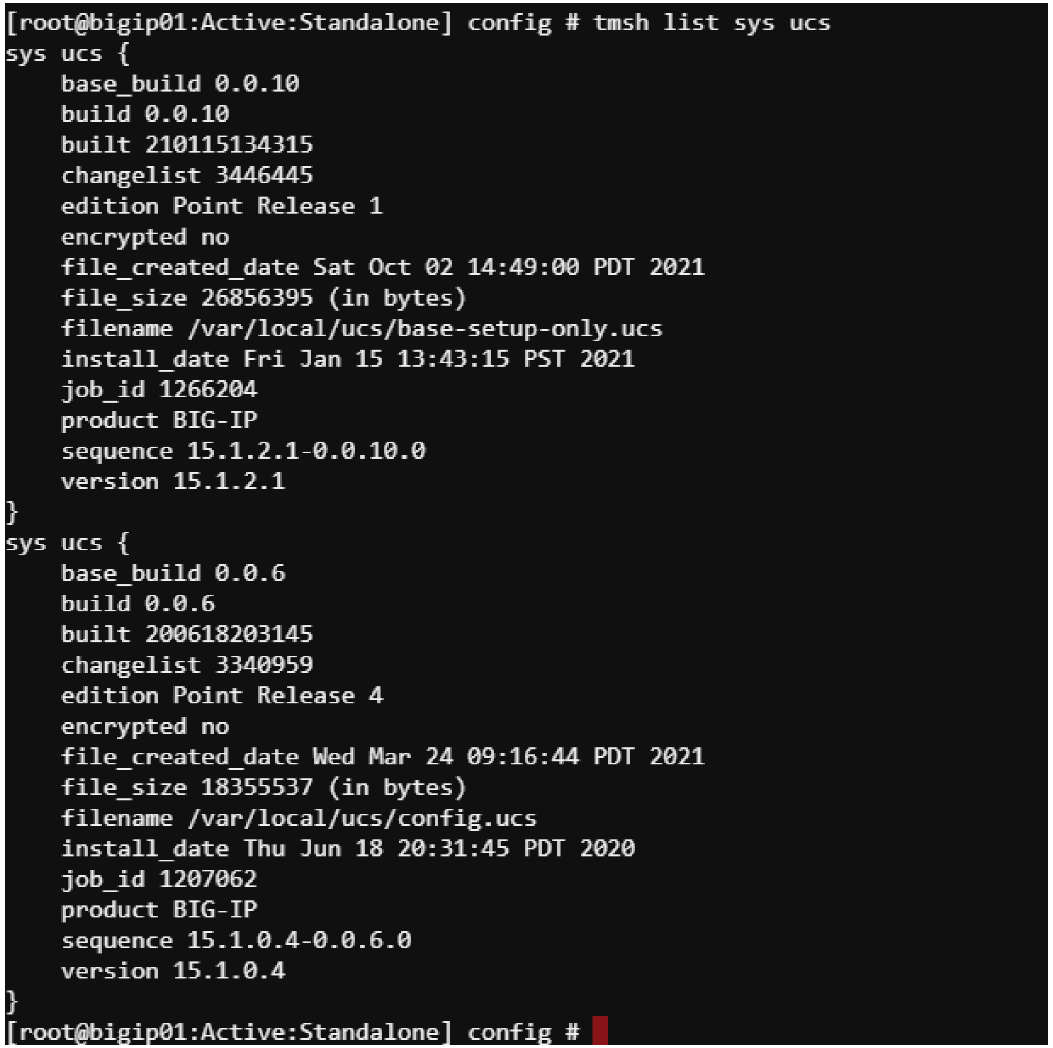
### Archive list

By default, the BIG-IP system saves the UCS archive file with a .ucs extension, if you do not include the extension in the file name. You can also specify a full path to the archive file, and then the system saves the archive file to the specified location. If you do not include a path, the system saves the file to the default archive directory, **/var/local/ucs**.

Archives that you locate in a directory other than the default directory do not appear in the list of available archives when you use the Configuration utility or the **list /sys ucs** command in **tmsh** to create or restore a UCS archive.

To easily identify the file, F5 recommends that you include the BIG-IP host name and current time stamp as part of the file name. For example:

tmsh save sys ucs $(echo $HOSTNAME | cut -d'.' -f1)-$(date +%H%M-%m%d%y)



```
[root@bigip01:Active:Standalone] config # tmsh list sys ucs
sys ucs {
    base_build 0.0.10
    build 0.0.10
    built 210115134315
    changelist 3446445
    edition Point Release 1
    encrypted no
    file_created_date Sat Oct 02 14:49:00 PDT 2021
    file_size 26856395 (in bytes)
    filename /var/local/ucs/base-setup-only.ucs
    install_date Fri Jan 15 13:43:15 PST 2021
    job_id 1266204
    product BIG-IP
    sequence 15.1.2.1-0.0.10.0
    version 15.1.2.1
}
sys ucs {
    base_build 0.0.6
    build 0.0.6
    built 200618203145
    changelist 3340959
    edition Point Release 4
    encrypted no
    file_created_date Wed Mar 24 09:16:44 PDT 2021
    file_size 18355537 (in bytes)
    filename /var/local/ucs/config.ucs
    install_date Thu Jun 18 20:31:45 PDT 2020
    job_id 1207062
    product BIG-IP
    sequence 15.1.0.4-0.0.6.0
    version 15.1.0.4
}
[root@bigip01:Active:Standalone] config #
```

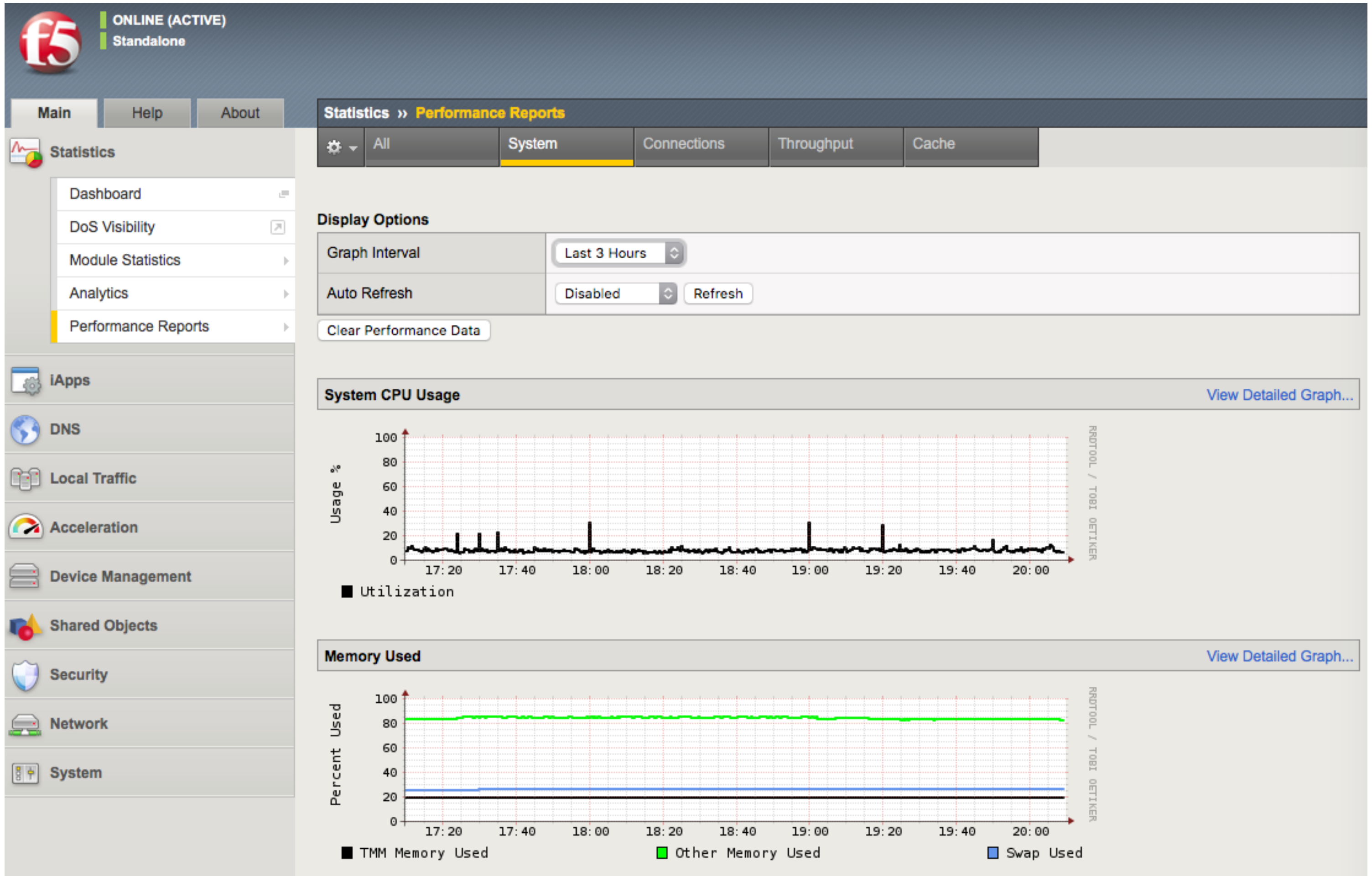
# Objective 3.05

## Review system vitals (disk space, CPU load, memory, bandwidth)

With the Application Visibility and Reporting (AVR) module, you can view BIG-IP System Vitals including:

- Internet Protocol (IP) packets, errors, and fragments
- Virtual server traffic details, TCP traffic, and UDP traffic
- CPU usage
- CPU utilization per process
- Memory statistics for TMM, other processes, system RAM, and swap space
- Disk activity, sizes, and latency

Manual Chapter : Viewing System-Level Statistics – [https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-analytics-implementations-14-1-0/viewing-system-level-statistics.html](https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-analytics-implementations-14-1-0/viewing-system-level-statistics.html)



Display Options

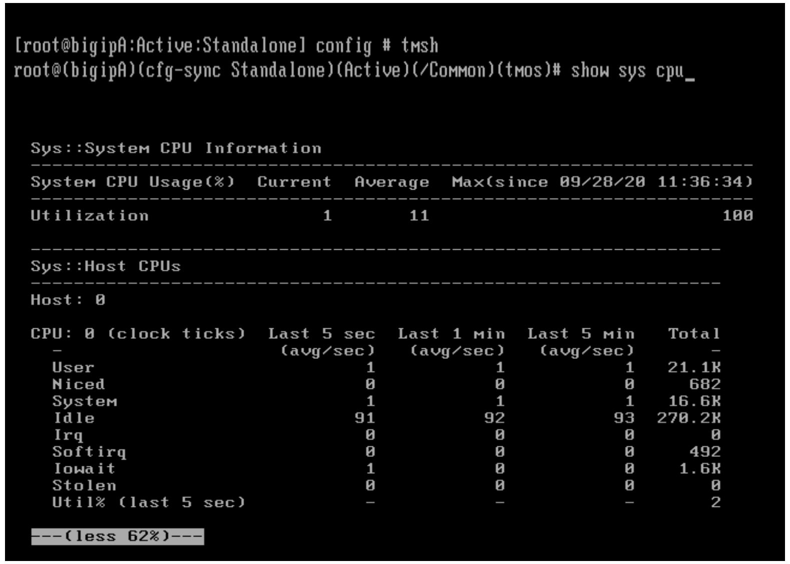
| | |
|---|---|
| Graph Interval | Last 3 Hours |
| Auto Refresh | Disabled |

System CPU Usage

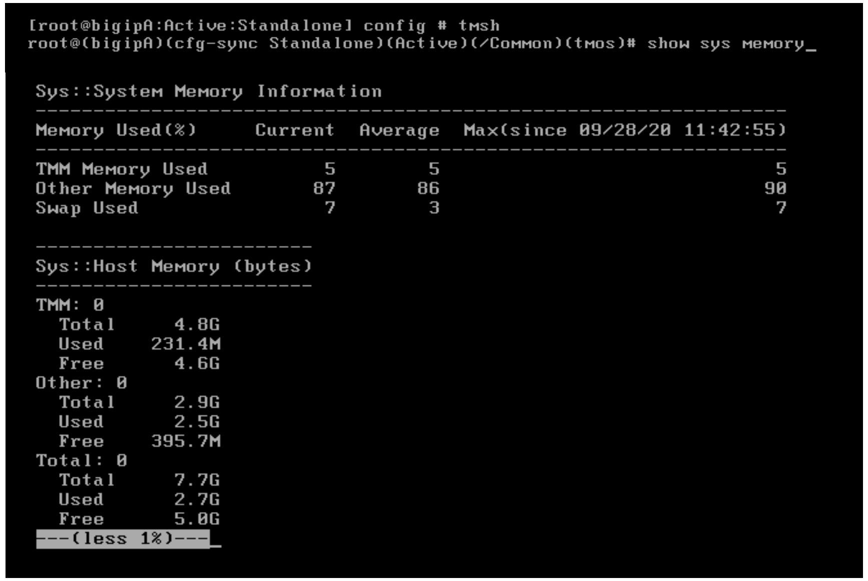
Memory Used

# Objective 3.05

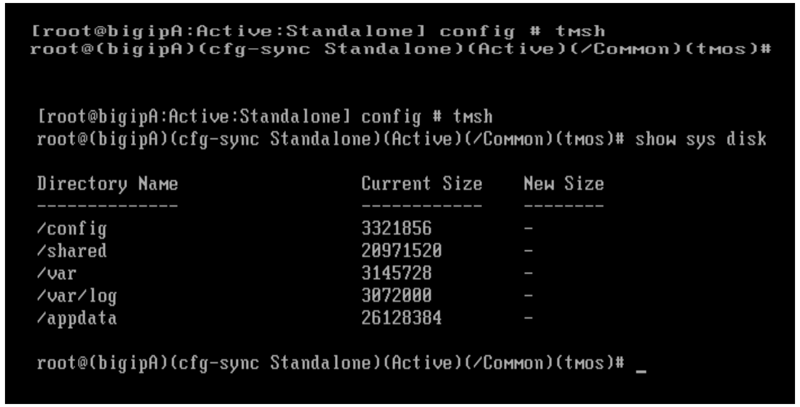
Review system vitals (disk space, CPU load, memory, bandwidth)



```
[root@bigipA:Active:Standalone] config # tmsh
root@(bigipA)(cfg-sync Standalone)(Active)(/Common)(tmos)# show sys cpu_


  Sys::System CPU Information
  ---------------------------------------------------------------------
  System CPU Usage(%)  Current  Average  Max(since 09/28/20 11:36:34)
  ---------------------------------------------------------------------
  Utilization                1       11                           100

  ------------------------------------------------------------------
  Sys::Host CPUs
  ------------------------------------------------------------------
  Host: 0

  CPU: 0 (clock ticks)  Last 5 sec  Last 1 min  Last 5 min    Total
    -                    (avg/sec)   (avg/sec)   (avg/sec)        -
    User                         1           1           1    21.1K
    Niced                        0           0           0      682
    System                       1           1           1    16.6K
    Idle                        91          92          93   270.2K
    Irq                          0           0           0        0
    Softirq                      0           0           0      492
    Iowait                       1           0           0     1.6K
    Stolen                       0           0           0        0
    Util% (last 5 sec)           -           -           -        2

  ---(less 62%)---
```



```
[root@bigipA:Active:Standalone] config # tmsh
root@(bigipA)(cfg-sync Standalone)(Active)(/Common)(tmos)# show sys memory_

 Sys::System Memory Information
 ----------------------------------------------------------------
 Memory Used(%)      Current  Average  Max(since 09/28/20 11:42:55)
 ----------------------------------------------------------------
 TMM Memory Used           5        5                            5
 Other Memory Used        87       86                           90
 Swap Used                 7        3                            7

 ------------------------
 Sys::Host Memory (bytes)
 ------------------------
 TMM: 0
   Total      4.8G
   Used     231.4M
   Free       4.6G
 Other: 0
   Total      2.9G
   Used       2.5G
   Free     395.7M
 Total: 0
   Total      7.7G
   Used       2.7G
   Free       5.0G
 ---(less 1%)---_
```



```
[root@bigipA:Active:Standalone] config # tmsh
root@(bigipA)(cfg-sync Standalone)(Active)(/Common)(tmos)#


[root@bigipA:Active:Standalone] config # tmsh
root@(bigipA)(cfg-sync Standalone)(Active)(/Common)(tmos)# show sys disk

Directory Name                 Current Size  New Size
--------------                 ------------  --------
/config                        3321856       -
/shared                        20971520      -
/var                           3145728       -
/var/log                       3072000       -
/appdata                       26128384      -

root@(bigipA)(cfg-sync Standalone)(Active)(/Common)(tmos)# _
```

## EXAM DETAILS

**How much do F5 exams cost?**
All F5 exams are currently priced at $180 USD (not including local taxes and fees) per exam, per attempt.

**How long are F5 exams?**
Most F5 exams are 90-minutes long, by default (not including any non-native English or other accommodations).

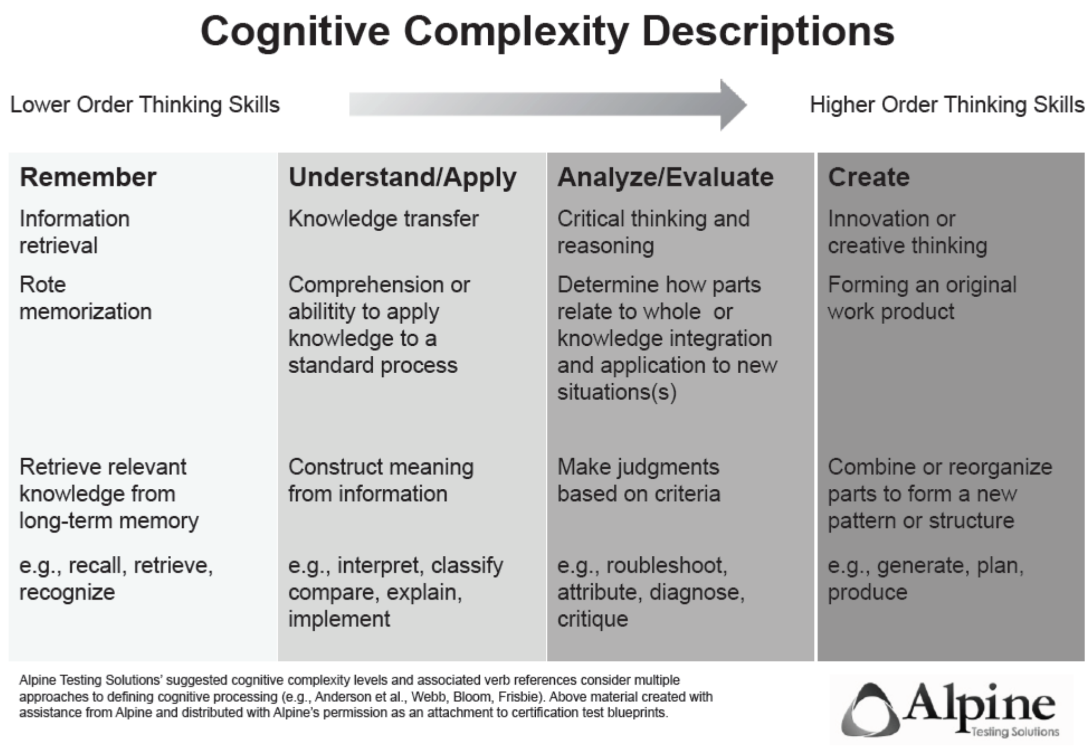
**What is the passing score for F5 exams?**
F5 Exams require a passing score of **245** out of a range between 0 and 350.

**How many questions are there?**
Most F5 exams have 80 questions (70 items that are scored, and 10 pilot/beta items).

**What format are F5 exams?**
F5 Exams are all computer-based, multiple choice response exams. Some questions contain exhibits or scenarios that you will have to view to answer the question.

**What is the F5 retake policy?**
1st failure: Exam hold for 15-days (you cannot take the exam again for 15-days);
2nd failure: Exam hold for 30-days;
3rd failure: Exam hold for 45-days;
4th failure: Exam hold for or 365-days;
5th and subsequent failed attempts: 90-days.

The retake count is only reset when the exam is passed.



## Cognitive Complexity Descriptions

Lower Order Thinking Skills → Higher Order Thinking Skills

| **Remember** | **Understand/Apply** | **Analyze/Evaluate** | **Create** |
|---|---|---|---|
| Information retrieval | Knowledge transfer | Critical thinking and reasoning | Innovation or creative thinking |
| Rote memorization | Comprehension or abilitity to apply knowledge to a standard process | Determine how parts relate to whole or knowledge integration and application to new situations(s) | Forming an original work product |
| Retrieve relevant knowledge from long-term memory | Construct meaning from information | Make judgments based on criteria | Combine or reorganize parts to form a new pattern or structure |
| e.g., recall, retrieve, recognize | e.g., interpret, classify compare, explain, implement | e.g., roubleshoot, attribute, diagnose, critique | e.g., generate, plan, produce |

Alpine Testing Solutions' suggested cognitive complexity levels and associated verb references consider multiple approaches to defining cognitive processing (e.g., Anderson et al., Webb, Bloom, Frisbie). Above material created with assistance from Alpine and distributed with Alpine's permission as an attachment to certification test blueprints.

Alpine Testing Solutions

App World 2024