CompTIA Network+ Exam N10-008

Lesson 12

Ensuring Network Availability

Objectives

- Explain the use of network management services
- Use event management to ensure network availability
- Use performance metrics to ensure network availability

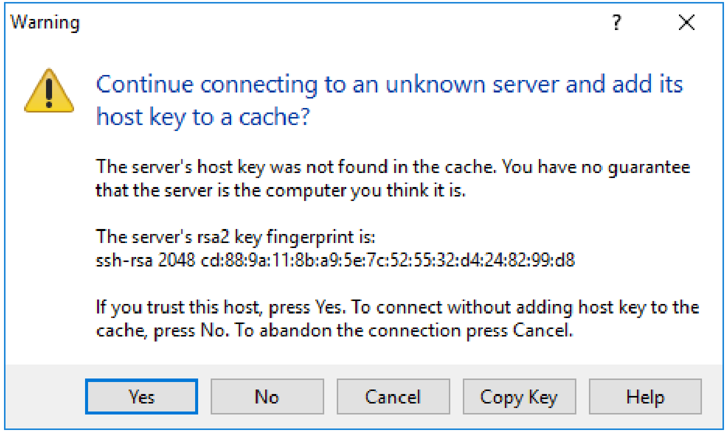
Lesson 12

Topic 12A

Explain the Use of Network Management Services

Secure Shell Servers and Terminal Emulators

- Command line terminal emulation
- Secure Shell (SSH)
  - Secure terminal emulation over port TCP/22
  - Tunnel other traffic over SSH
- Server authenticated by a host key
- Client authentication
  - User name/password
  - Public key authentication
  - Kerberos
- Ensure secure management of keys used for non-interactive logon



Continue connecting to an unknown server and add its host key to a cache?

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

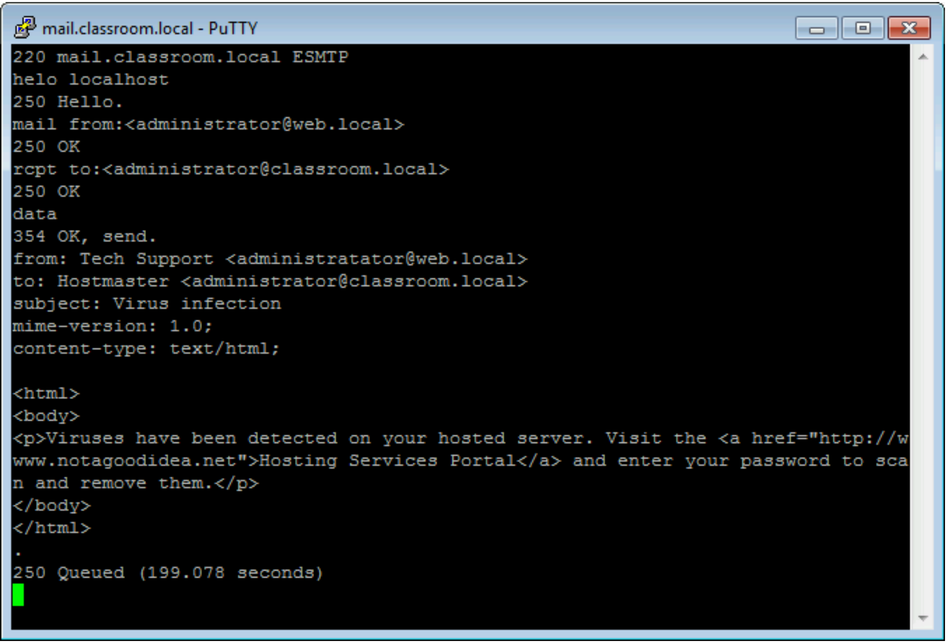
The server's rsa2 key fingerprint is:
ssh-rsa 2048 cd:88:9a:11:8b:a9:5e:7c:52:55:32:d4:24:82:99:d8

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

Secure Shell Commands

- sshd
- ssh-keygen
- ssh-agent
- ssh Host
- ssh Username@Host
- ssh Host “Command or Script”
- scp Username@Host:RemoteFile /Local/Destination
- sftp

Telnet



```
220 mail.classroom.local ESMTP
helo localhost
250 Hello.
mail from:<administrator@web.local>
250 OK
rcpt to:<administrator@classroom.local>
250 OK
data
354 OK, send.
from: Tech Support <administratator@web.local>
to: Hostmaster <administrator@classroom.local>
subject: Virus infection
mime-version: 1.0;
content-type: text/html;

<html>
<body>
<p>Viruses have been detected on your hosted server. Visit the <a href="http://w
www.notagoodidea.net">Hosting Services Portal</a> and enter your password to sca
n and remove them.</p>
</body>
</html>
.
250 Queued (199.078 seconds)
```

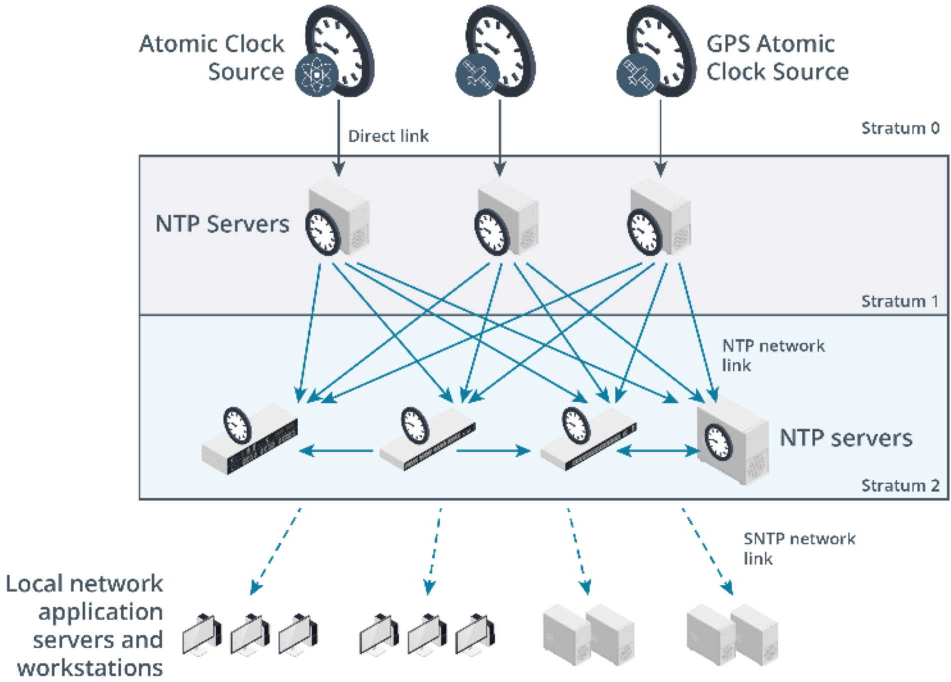
- Unsecure CLI terminal emulation over port TCP/23
- Plaintext protocol – no security
- Typically disabled

Remote Desktop Protocol

- GUI remote administration over TCP/3389
- Session can be encrypted
- Range of clients for different PC and mobile operating systems

Network Time Protocol

- Time critical services
  - Authentication, logging, task scheduling/backup, …
- Network Time Protocol (NTP)
  - Stratum 1 servers have direct physical link to accurate time source
  - Lower stratum servers sample multiple sources
  - Clients use simple NTP to obtain correct time
- Diagnosing errors due to incorrect time



Review Activity: Network Management Services

- Secure Shell Servers and Terminal Emulators
- Secure Shell Commands
- Telnet
- Remote Desktop Protocol
- Network Time Protocol

Lab Activity

Assisted Lab: Configure Secure Access Channels

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 12

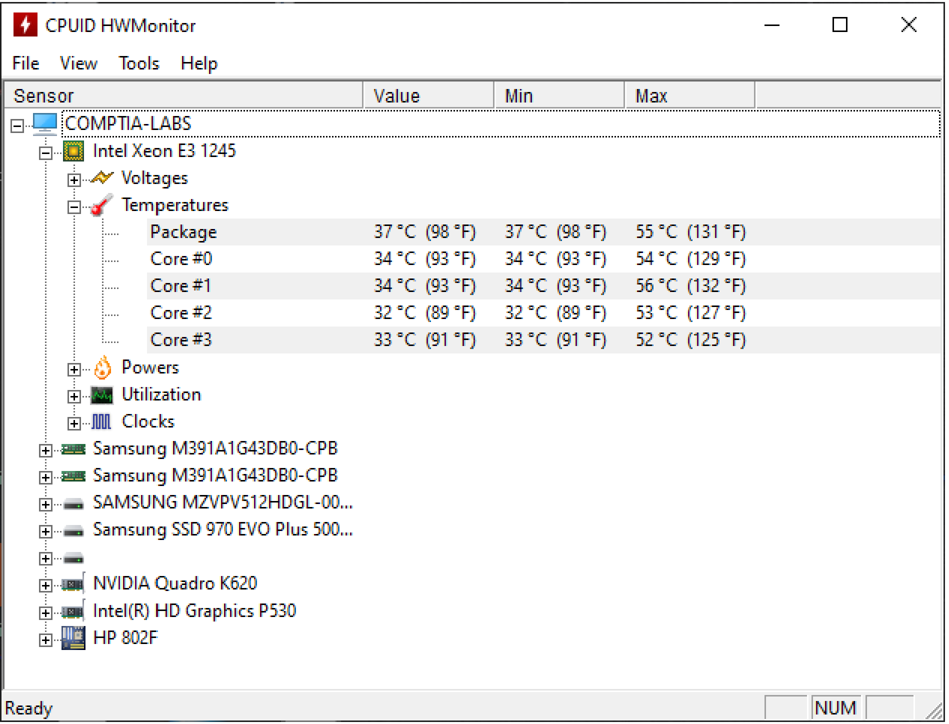
Topic 12B

Use Event Management to Ensure Network Availability

Performance Metrics, Bottlenecks, and Baselines

- Performance metrics
  - Bandwidth/throughput, CPU and memory resource, storage resource
- Bottlenecks
  - “Pinch points” that cause whole system to underperform
- Performance baselines
  - Record metrics as comparison
  - Update baselines

Environmental Monitoring

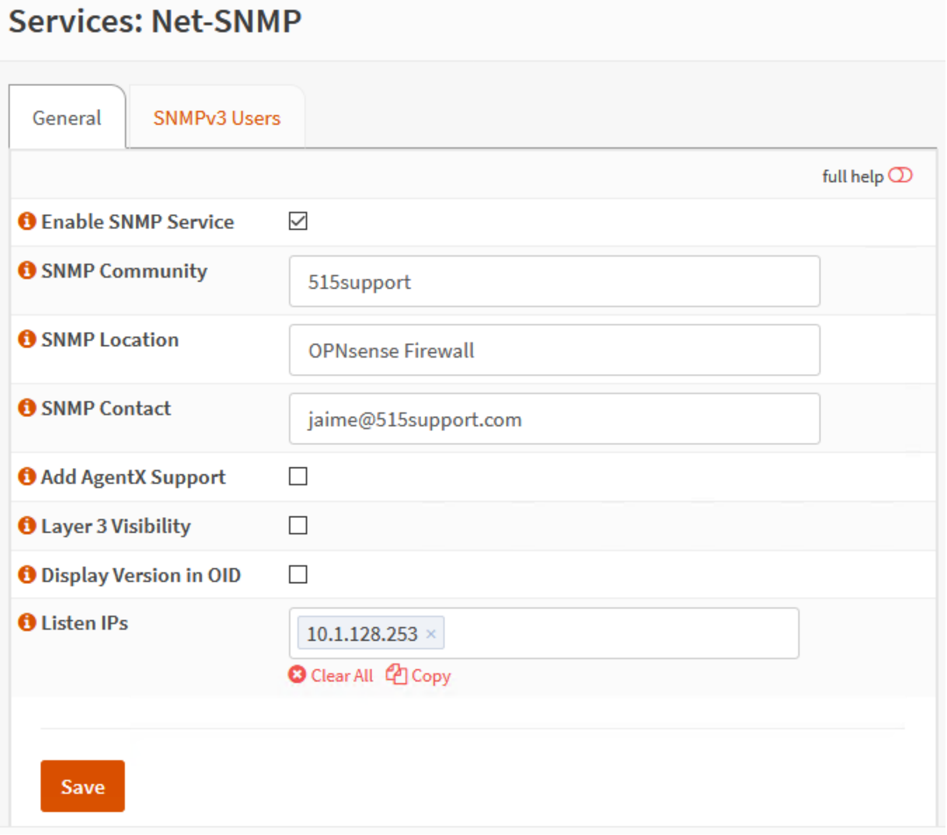


```
Sensor                          Value             Min               Max
COMPTIA-LABS
  Intel Xeon E3 1245
    Voltages
    Temperatures
      Package                   37 °C  (98 °F)    37 °C  (98 °F)    55 °C  (131 °F)
      Core #0                   34 °C  (93 °F)    34 °C  (93 °F)    54 °C  (129 °F)
      Core #1                   34 °C  (93 °F)    34 °C  (93 °F)    56 °C  (132 °F)
      Core #2                   32 °C  (89 °F)    32 °C  (89 °F)    53 °C  (127 °F)
      Core #3                   33 °C  (91 °F)    33 °C  (91 °F)    52 °C  (125 °F)
    Powers
    Utilization
    Clocks
  Samsung M391A1G43DB0-CPB
  Samsung M391A1G43DB0-CPB
  SAMSUNG MZVPV512HDGL-00...
  Samsung SSD 970 EVO Plus 500...

  NVIDIA Quadro K620
  Intel(R) HD Graphics P530
  HP 802F
```

- Environmental sensors detect factors that could affect integrity/reliability
- Device chassis sensors
  - Temperature, fan speed, voltage fluctuation, intrusion
- Ambient sensors
  - Temperature, humidity, electrical, flooding

Simple Network Management Protocol

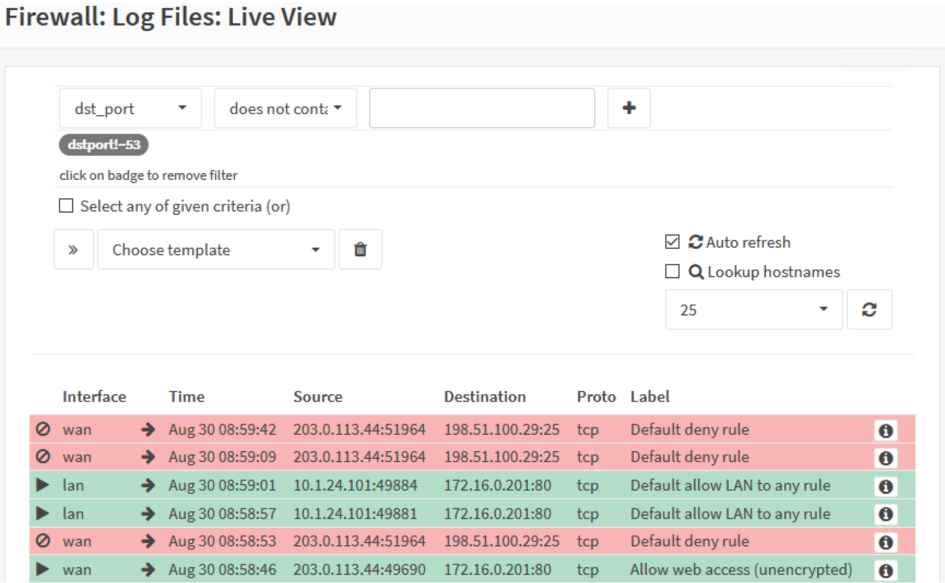
- Agents
  - Management Information Base (MIB)
  - Object Identifier (OID)
  - Community name
  - Read/only or read/write access
  - Traps
- SNMP monitor
  - Get, Trap, Walk
  - Ports UDP/161 (queries) and UDP/162 (traps)



Services: Net-SNMP

Enable SNMP Service	☑
SNMP Community	515support
SNMP Location	OPNsense Firewall
SNMP Contact	jaime@515support.com
Add AgentX Support	□
Layer 3 Visibility	□
Display Version in OID	□
Listen IPs	10.1.128.253 ×

Network Device Logs



Firewall: Log Files: Live View

dst_port | does not cont: | +

dstport!~53

click on badge to remove filter

☐ Select any of given criteria (or)

» Choose template

☑ Auto refresh

☐ Lookup hostnames

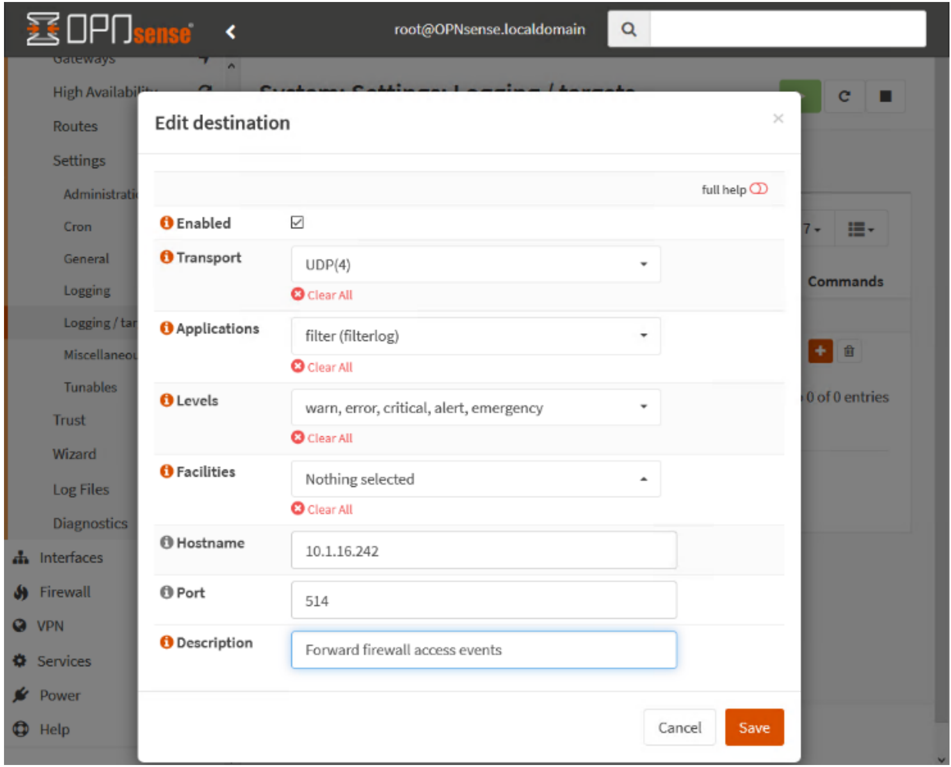
25

	Interface		Time	Source	Destination	Proto	Label
⊘	wan	→	Aug 30 08:59:42	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule
⊘	wan	→	Aug 30 08:59:09	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule
▶	lan	→	Aug 30 08:59:01	10.1.24.101:49884	172.16.0.201:80	tcp	Default allow LAN to any rule
▶	lan	→	Aug 30 08:58:57	10.1.24.101:49881	172.16.0.201:80	tcp	Default allow LAN to any rule
⊘	wan	→	Aug 30 08:58:53	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule
▶	wan	→	Aug 30 08:58:46	203.0.113.44:49690	172.16.0.201:80	tcp	Allow web access (unencrypted)

- Performance, troubleshooting, and security (auditing) information
  - Metadata plus event description
- Log types
  - System and application logs
  - Audit logs
  - Performance/traffic logs

Log Collectors and Syslog

- Centralized collection of events from multiple sources
- Syslog protocol for forwarding over UDP/514
- Syslog open format for log messages
  - PRI code
  - Header
  - Message



Edit destination

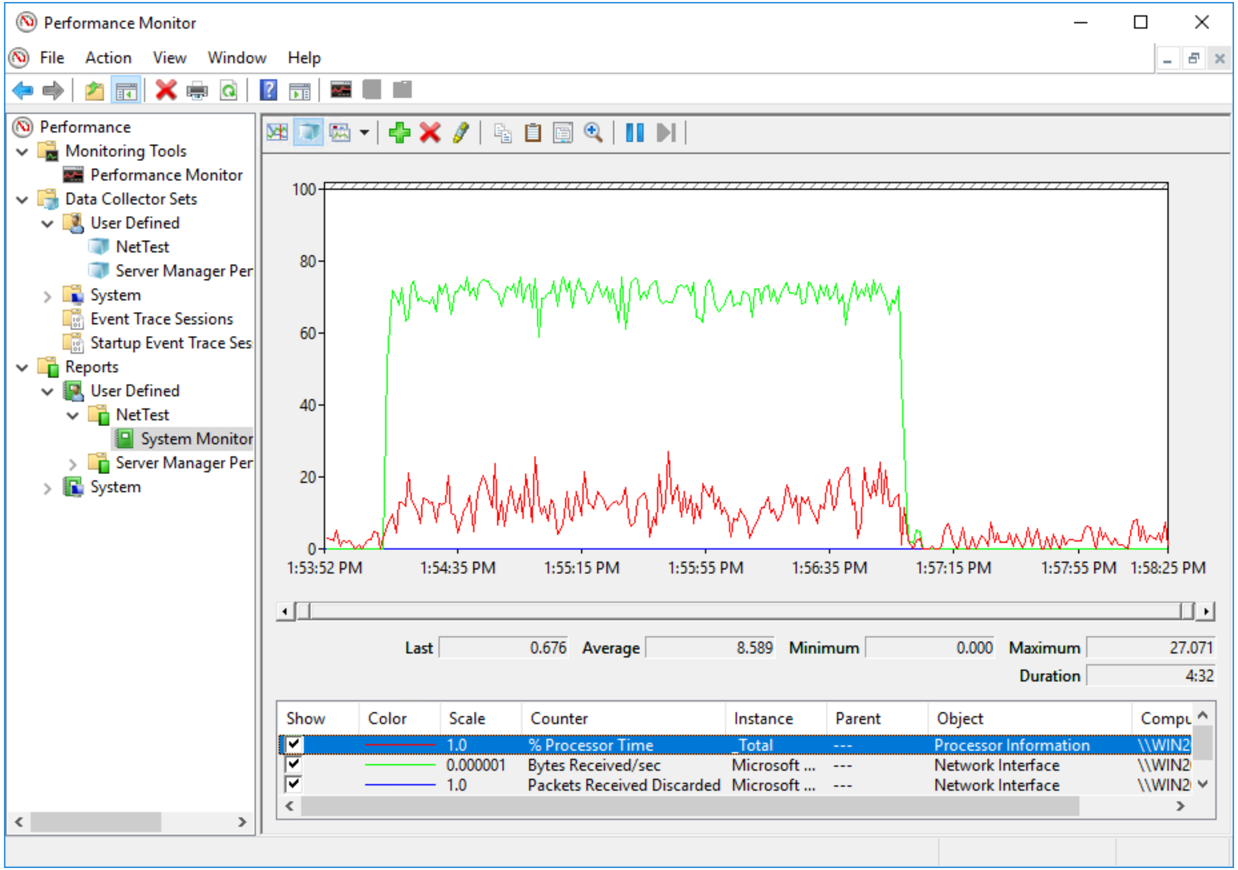
Enabled	☑
Transport	UDP(4)
Applications	filter (filterlog)
Levels	warn, error, critical, alert, emergency
Facilities	Nothing selected
Hostname	10.1.16.242
Port	514
Description	Forward firewall access events

Event Management

- Event categorization
- Windows
  - Informational, warning, or critical
  - Audit success or fail
- Syslog severity levels
  - 0 (emergency) down to 7 (debug)
- Logging level and alert configuration
  - Threshold
  - Alert versus notifications and alarms
  - Ticket systems

Log Reviews

- Monitoring versus review/analysis
- Trends
- Graphing



Last 0.676 Average 8.589 Minimum 0.000 Maximum 27.071
Duration 4:32

Show	Color	Scale	Counter	Instance	Parent	Object	Compu
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\WIN2
☑	🟩	0.000001	Bytes Received/sec	Microsoft ...	---	Network Interface	\\WIN2
☑	🟦	1.0	Packets Received Discarded	Microsoft ...	---	Network Interface	\\WIN2

Review Activity: Event Management

- Performance Metrics, Bottlenecks, and Baselines
- Environmental Monitoring
- Simple Network Management Protocol
- Network Device Logs
- Log Collectors and Syslog
- Event Management
- Log Reviews

Lab Activity

Assisted Lab: Configure Syslog

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 12

Topic 12C

Use Performance Metrics to Ensure Network Availability

Network Metrics

- Application requirements for high bandwidth and sensitivity to delay
- Bandwidth
  - Speed, throughput, and goodput
  - Calculating requirements for audio and video
- Latency and jitter
  - Signal delay measured in milliseconds (ms)
  - Variation in delay
  - Measurement tools (pathping and mtr)
  - One-way versus Round Trip Time (RTT)

Bandwidth Management

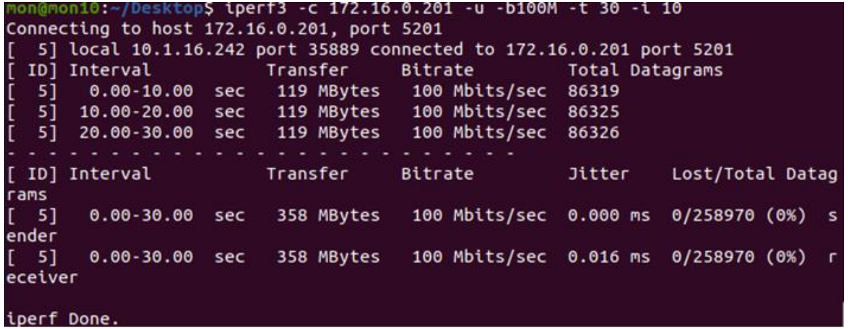
- Provision higher bandwidth links or prioritize traffic classes
- Differentiated Services (DiffServ)
  - Type of Service field in the IPv4 header/Traffic Class in IPv6
  - 6-byte DiffServ Code Point (DSCP)
- IEEE 802.1p
  - 3-bit priority field in 802.1Q VLAN header
  - Mapping DSCP to 802.1p
    - Network control (highest priority)
    - Expedited forwarding
    - Assured forwarding
    - Best effort (lowest priority)

Traffic Shaping

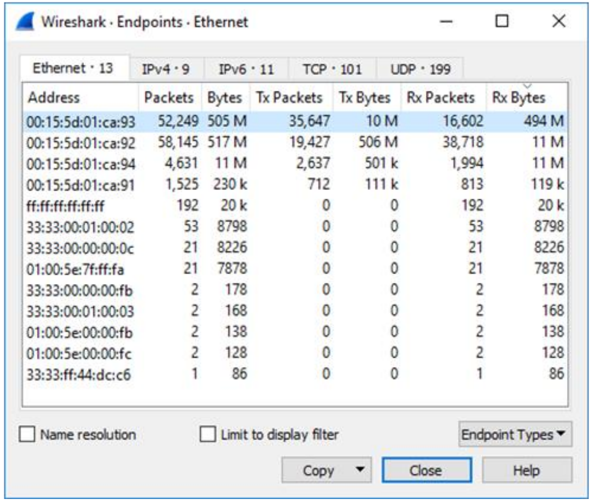
- Quality of Service (QoS) versus Class of Service (CoS)
  - Privilege real-time data over bursty data
  - CoS tags data with priority type
  - QoS allows control over network link parameters
  - Multiprotocol Label Switching (MPLS)
- Traffic policing enforces bandwidth limits
- Traffic shaping
  - Reserve link bandwidth
  - Prioritize traffic
  - Filter/deprioritize unwanted traffic

Traffic Analysis Tools

- Throughput testers
  - Assess goodput
  - iperf
- Top talkers/listeners
- Bandwidth speed testers
  - Broadband speed checkers
  - Test website performance/ monitor availability



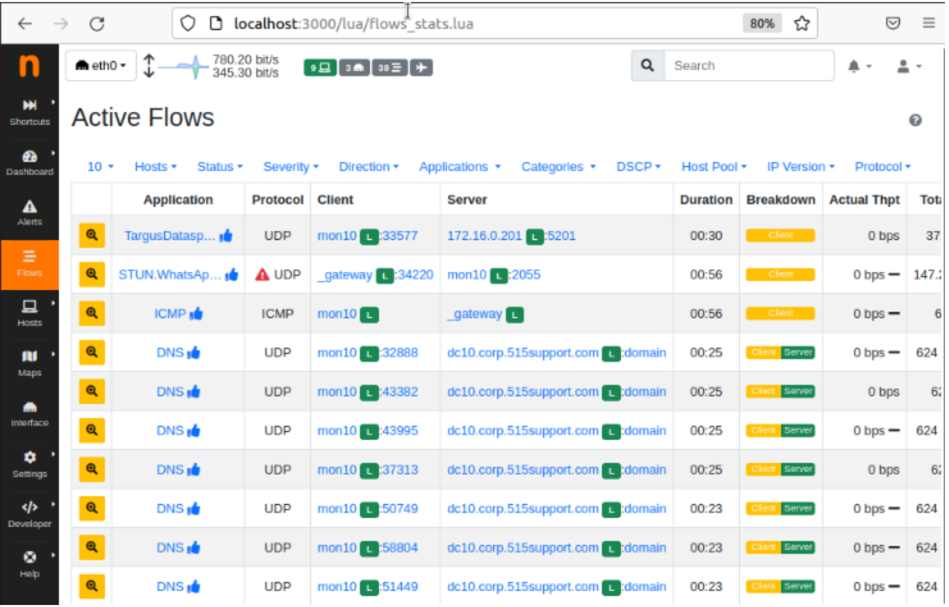
```
mon@mon10:~/Desktop$ iperf3 -c 172.16.0.201 -u -b100M -t 30 -i 10
Connecting to host 172.16.0.201, port 5201
[  5] local 10.1.16.242 port 35889 connected to 172.16.0.201 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-10.00  sec   119 MBytes   100 Mbits/sec  86319
[  5]  10.00-20.00  sec   119 MBytes   100 Mbits/sec  86325
[  5]  20.00-30.00  sec   119 MBytes   100 Mbits/sec  86326
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datag
rams
[  5]   0.00-30.00  sec   358 MBytes   100 Mbits/sec  0.000 ms  0/258970 (0%)  s
ender
[  5]   0.00-30.00  sec   358 MBytes   100 Mbits/sec  0.016 ms  0/258970 (0%)  r
eceiver

iperf Done.
```



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:15:5d:01:ca:93	52,249	505 M	35,647	10 M	16,602	494 M
00:15:5d:01:ca:92	58,145	517 M	19,427	506 M	38,718	11 M
00:15:5d:01:ca:94	4,631	11 M	2,637	501 k	1,994	11 M
00:15:5d:01:ca:91	1,525	230 k	712	111 k	813	119 k
ff:ff:ff:ff:ff:ff	192	20 k	0	0	192	20 k
33:33:00:01:00:02	53	8798	0	0	53	8798
33:33:00:00:00:0c	21	8226	0	0	21	8226
01:00:5e:7f:ff:fa	21	7878	0	0	21	7878
33:33:00:00:00:fb	2	178	0	0	2	178
33:33:00:01:00:03	2	168	0	0	2	168
01:00:5e:00:00:fb	2	138	0	0	2	138
01:00:5e:00:00:fc	2	128	0	0	2	128
33:33:ff:44:dc:c6	1	86	0	0	1	86

☐ Name resolution ☐ Limit to display filter

Netflow



Active Flows

	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Tot
🔍	TargusDatasp... 👍	UDP	mon10 L :33577	172.16.0.201 L :5201	00:30	Client	0 bps	37
🔍	STUN.WhatsAp... 👍	⚠ UDP	_gateway L :34220	mon10 L :2055	00:56	Client	0 bps —	147.
🔍	ICMP 👍	ICMP	mon10 L	_gateway L	00:56	Client	0 bps —	6
🔍	DNS 👍	UDP	mon10 L :32888	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps —	624
🔍	DNS 👍	UDP	mon10 L :43382	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps	62
🔍	DNS 👍	UDP	mon10 L :43995	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps —	624
🔍	DNS 👍	UDP	mon10 L :37313	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps	62
🔍	DNS 👍	UDP	mon10 L :50749	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624
🔍	DNS 👍	UDP	mon10 L :58804	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624
🔍	DNS 👍	UDP	mon10 L :51449	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624

- Gather traffic metadata only and report it to a structured database
- NetFlow and IP Flow Information Export (IPFIX) IETF standard
- NetFlow exporters
  - Traffic flow defined by packets that share the same characteristics
  - 5-tuple and 7-tuple
- NetFlow collectors
- NetFlow analyzers

Interface Monitoring Metrics

- Link state
  - Uptime and downtime
- Resets
- Speed
- Duplex

- Utilization
  - Send versus receive
  - Bits per second or percentage of link bandwidth
  - Overall versus peak
- Per-protocol utilization
  - Packet/byte counts
- Error rate
- Discards/drops
- Retransmissions

Troubleshooting Interface Errors

- Cyclic Redundancy Check (CRC) errors
- Encapsulation errors
  - Frame type
  - Ethernet trunks
  - WAN framing
- Runt Frame errors
- Giant Frame errors

Review Activity: Performance Metrics

- Network Metrics
- Bandwidth Management
- Traffic Shaping
- Traffic Analysis Tools
- Netflow
- Interface Monitoring Metrics
- Troubleshooting Interface Errors

Lab Activity

Assisted Lab: Analyze Network Performance

Applied Lab: Verify Service and Application Configuration

- Lab types
    - Assisted labs guide you step-by-step through tasks
    - Applied labs set goals with limited guidance
- Complete lab
    - Submit all items for grading and check each progress box
    - Select “Grade Lab” from final page
- Save lab
    - Select the hamburger menu and select “Save”
    - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
    - Select the hamburger menu and select “End”

CompTIA Network+ Exam N10-008

Lesson 12

Summary