ComNetLab

Vaan Megam Networks

Empowering Connectivity,
Enhancing Security

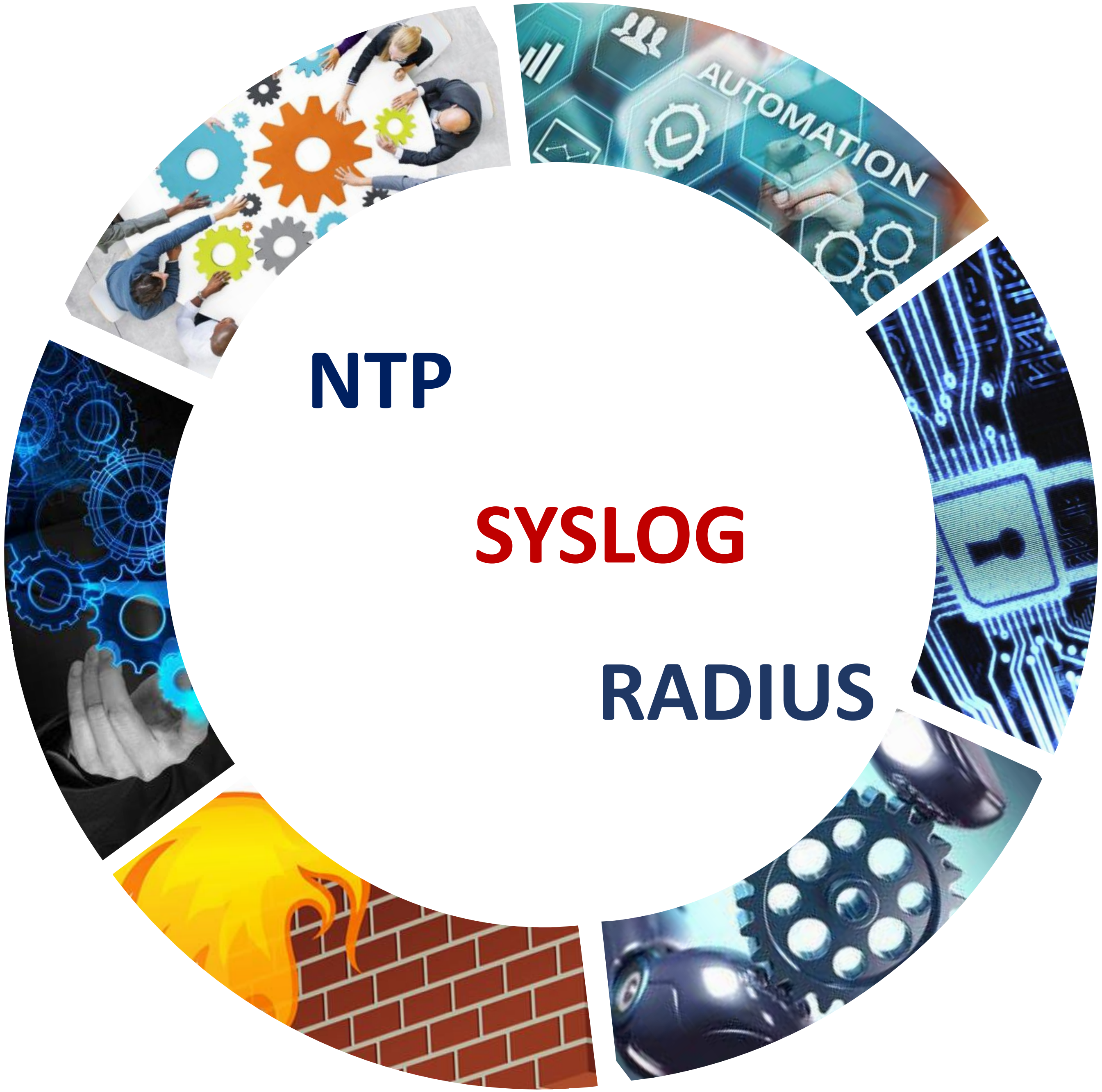
EXTERNAL ADJUNCTS

Nagarajan Senguttuvan

Senior Network Architect

CCIE # EI (51816), PCNSE

Members of: ONF 3GPP A GLOBAL INITIATIVE oneM2M The IoT Standard tsdsi

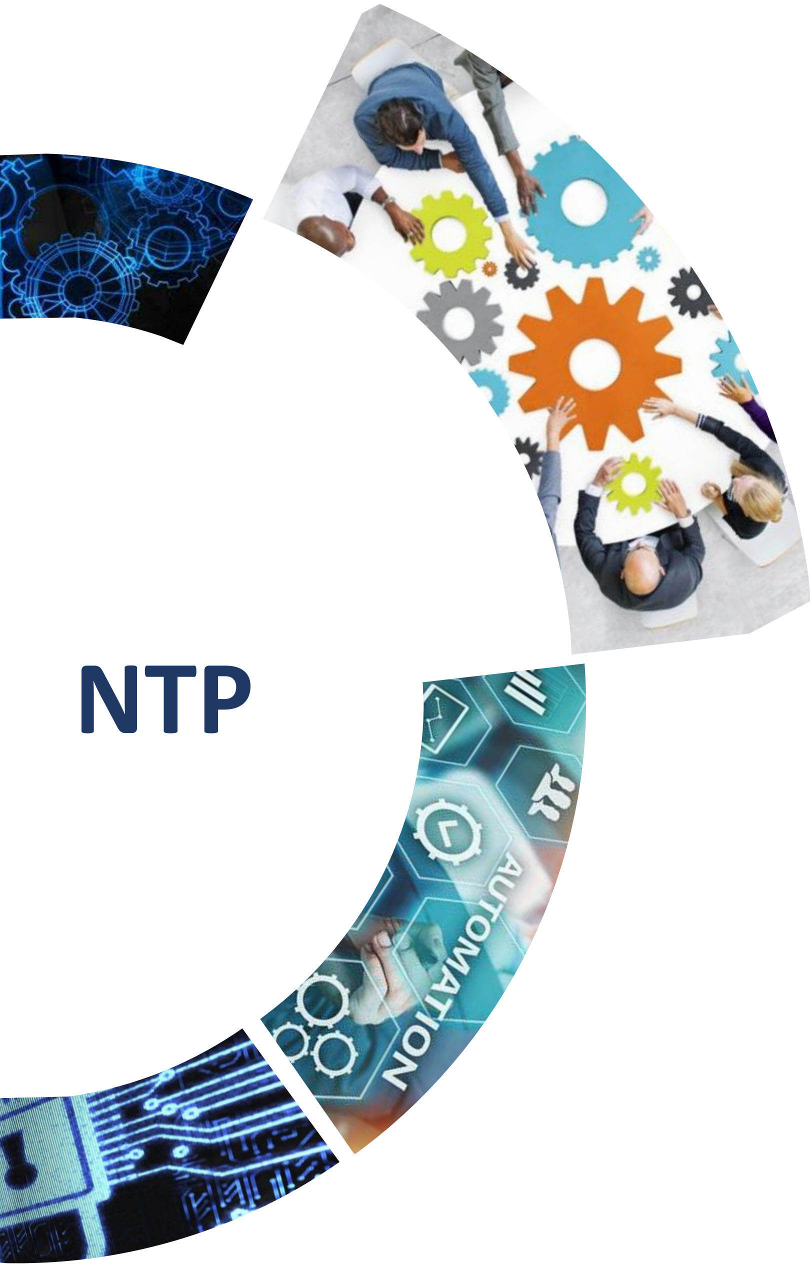


NTP

SYSLOG

RADIUS

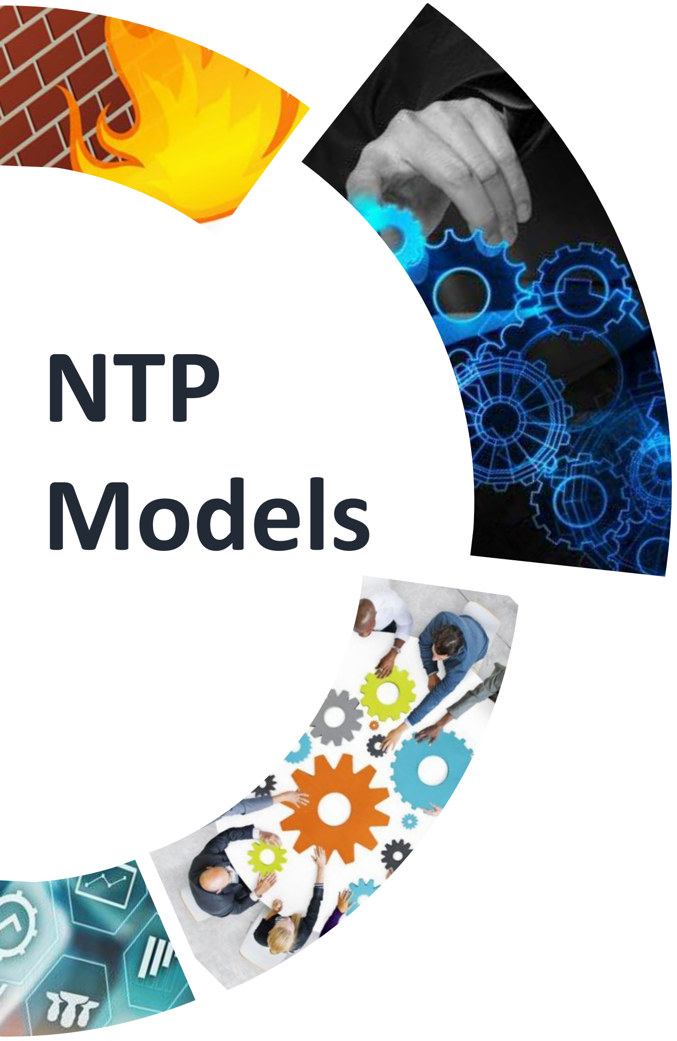
NTP



- Network Time Protocol (NTP) is essential for keeping clocks on a network synchronized with Coordinated Universal Time (UTC) within a few milliseconds.
- It operates over User Datagram Protocol (UDP) on port 123, exchanging timestamp data.
- NTP can function in either a client-server model or a peer-to-peer configuration.
- The table highlights the critical areas where accurate network timekeeping is essential for both network operations and various applications

Log file accuracy, auditing, and monitoring	**Transaction processing**
Network fault diagnosis and recovery	Email
Virtual environments	Legal and regulatory requirements
Directory services	Scheduled operations
Access security and authentication	Real-world time values

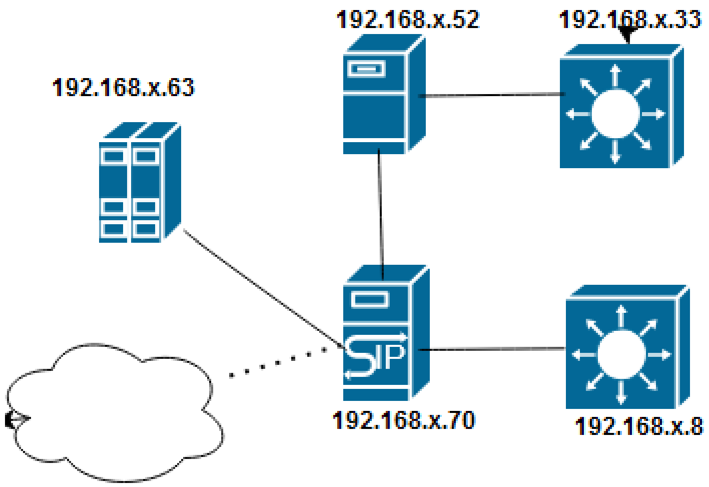
Vaan Megam
Networks

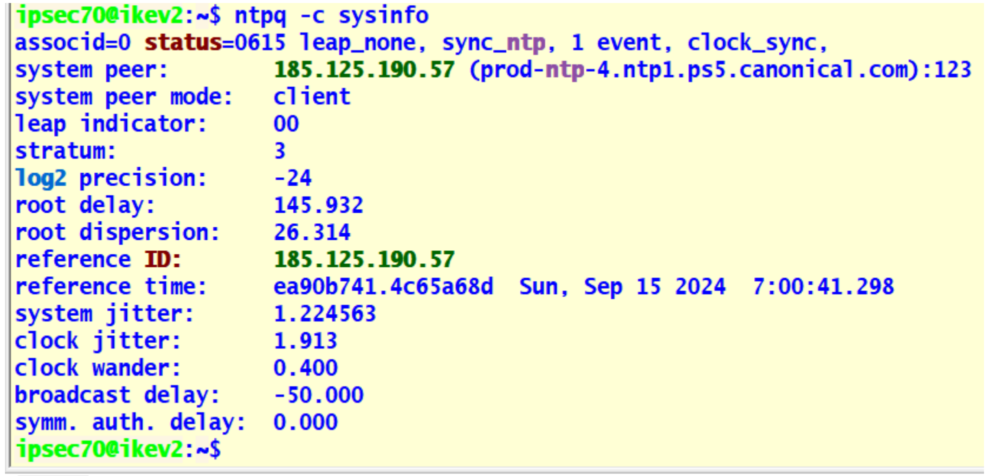


NTP Models

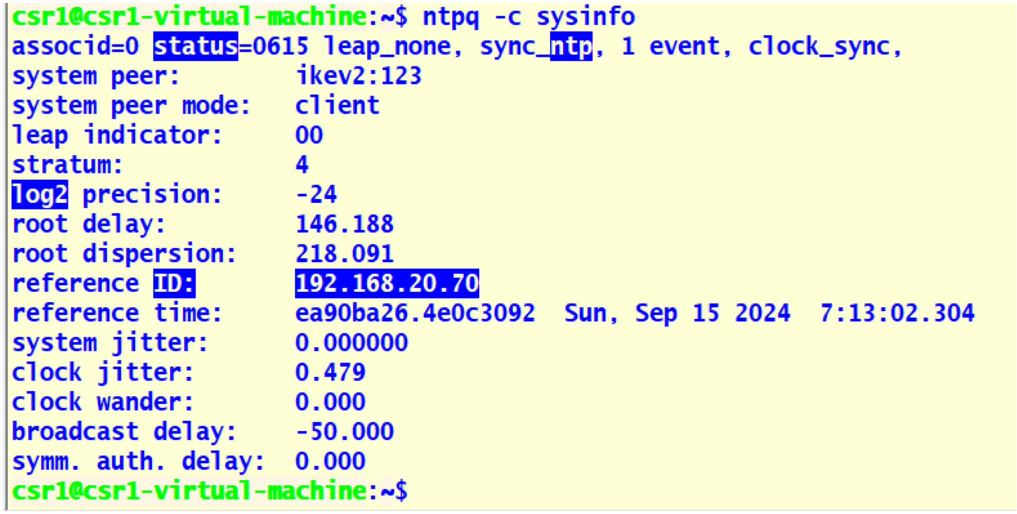
- NTP operates in a stratum-based hierarchy, with each device assigned a stratum level based on its distance from a reference clock.
- Stratum 0:Reference clocks such as atomic clocks, GPS receivers, or radio clocks, which provide highly accurate time.
- Stratum 1: Servers directly connected to Stratum 0 devices. They distribute time to lower-stratum devices.
- Stratum 2 and below Servers or clients that synchronize their time from Stratum 1 servers. Each successive level communicates with the level above for time updates.
- NTP Servers: These are higher-stratum devices (usually Stratum 1 or 2) that provide accurate time to other devices on the network.NTP Clients: These devices request time from NTP servers and adjust their clocks based on the received data.
- Client-Server Model: NTP client sends a request to an NTP server, receives the time, and adjusts its clock accordingly. The server doesn't need to initiate communication; it simply responds to client requests
- Peer-to-Peer Mode: NTP can also work in a peer-to-peer configuration where devices share time information with each other. This mode is useful for environments where no central NTP server exists, and devices synchronize mutually.

NTP - Demo

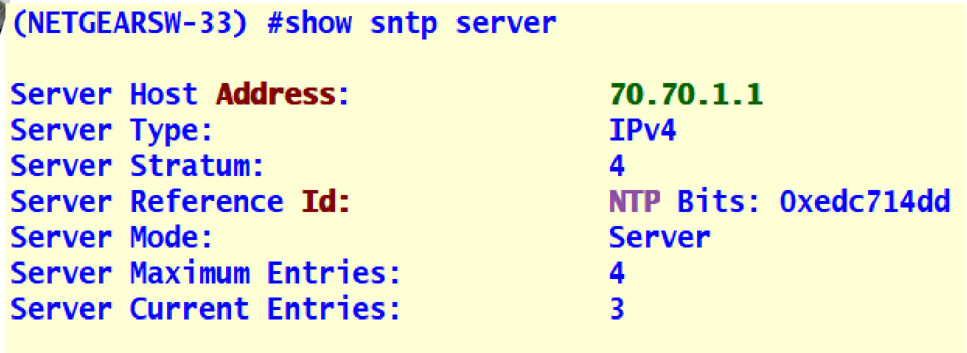




```
ipsec70@ikev2:~$ ntpq -c sysinfo
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:        185.125.190.57 (prod-ntp-4.ntp1.ps5.canonical.com):123
system peer mode:   client
leap indicator:     00
stratum:            3
log2 precision:     -24
root delay:         145.932
root dispersion:    26.314
reference ID:       185.125.190.57
reference time:     ea90b741.4c65a68d  Sun, Sep 15 2024  7:00:41.298
system jitter:      1.224563
clock jitter:       1.913
clock wander:       0.400
broadcast delay:    -50.000
symm. auth. delay:  0.000
ipsec70@ikev2:~$
```



```
csr1@csr1-virtual-machine:~$ ntpq -c sysinfo
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:        ikev2:123
system peer mode:   client
leap indicator:     00
stratum:            4
log2 precision:     -24
root delay:         146.188
root dispersion:    218.091
reference ID:       192.168.20.70
reference time:     ea90ba26.4e0c3092  Sun, Sep 15 2024  7:13:02.304
system jitter:      0.000000
clock jitter:       0.479
clock wander:       0.000
broadcast delay:    -50.000
symm. auth. delay:  0.000
csr1@csr1-virtual-machine:~$
```



```
(NETGEARSW-33) #show sntp server

Server Host Address:                      70.70.1.1
Server Type:                              IPv4
Server Stratum:                           4
Server Reference Id:                      NTP Bits: 0xedc714dd
Server Mode:                              Server
Server Maximum Entries:                   4
Server Current Entries:                   3
```

SNTP is a simplified version of NTP that's used when full NTP implementation isn't required.

Vaan Megam
Networks

SYSLOG

Syslog, or System Logging Protocol, is a standard for logging messages from computer systems to a central location, it helps track system health by recording and analyzing events and errors.

Syslog messages can be used for a variety of purposes, including security investigations, auditing, system management, and infrastructure maintenance.

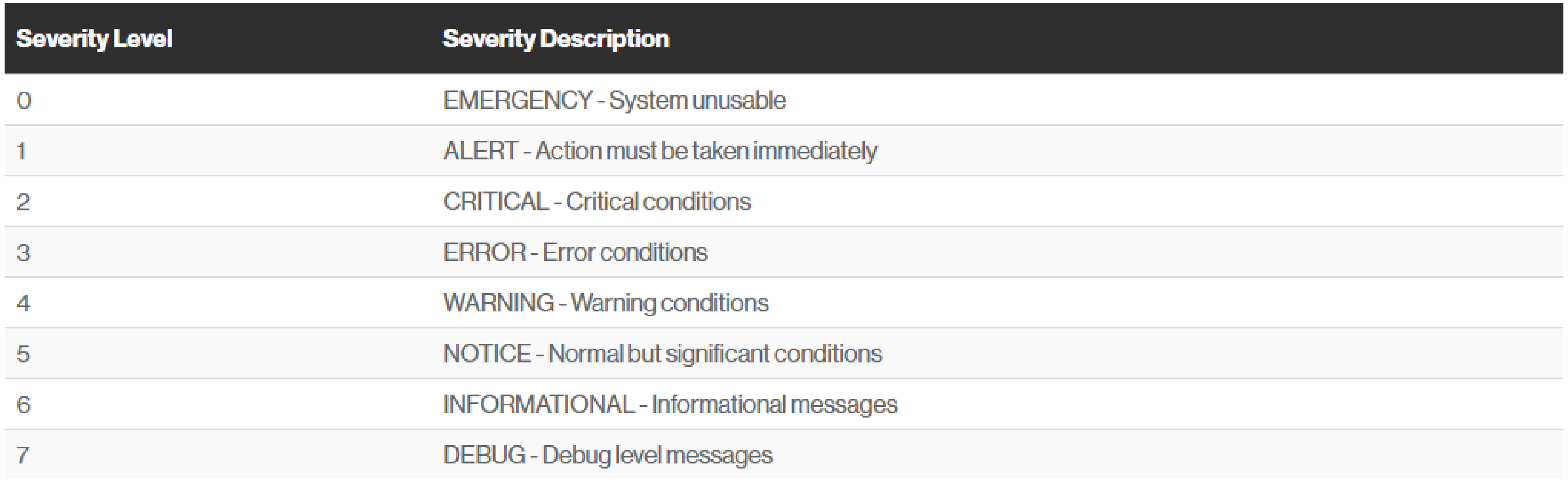
Components:

Syslog Clients: Devices generating logs (routers, switches, firewalls).

Syslog Server: Central log repository.

Log Analyzer: Tool for filtering, searching, and reporting.

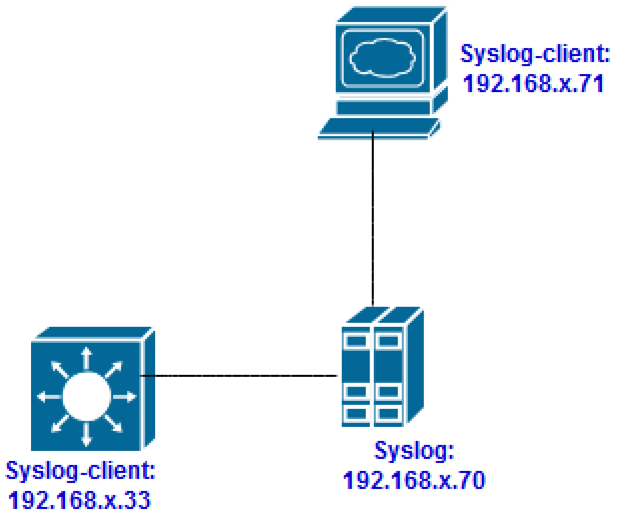
The severity level identifies the criticality level of the event and is useful for filtering events and determining alert action.

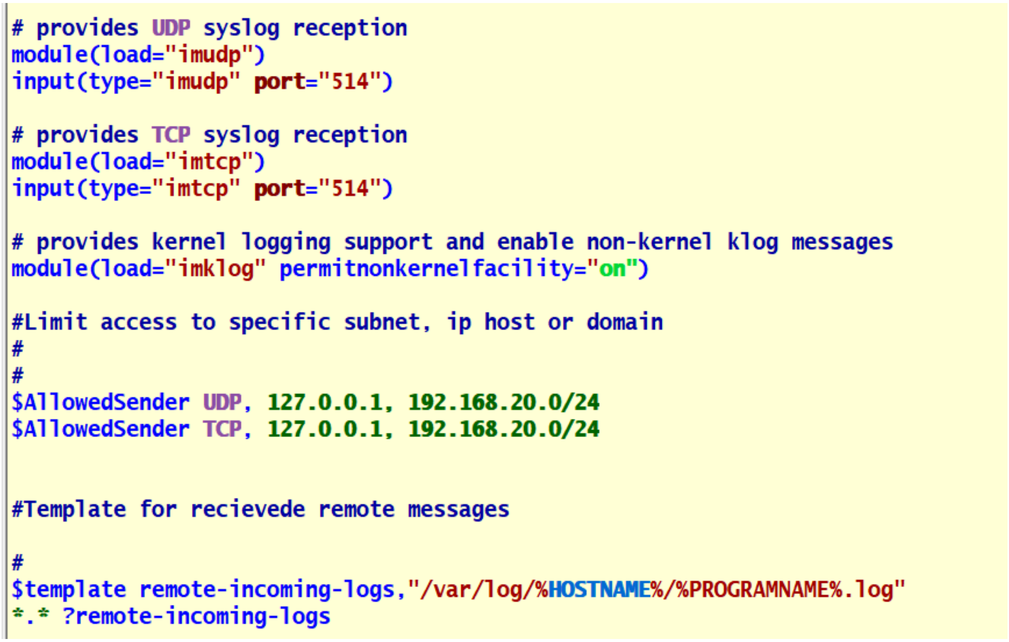


Severity Level	Severity Description
0	EMERGENCY - System unusable
1	ALERT - Action must be taken immediately
2	CRITICAL - Critical conditions
3	ERROR - Error conditions
4	WARNING - Warning conditions
5	NOTICE - Normal but significant conditions
6	INFORMATIONAL - Informational messages
7	DEBUG - Debug level messages

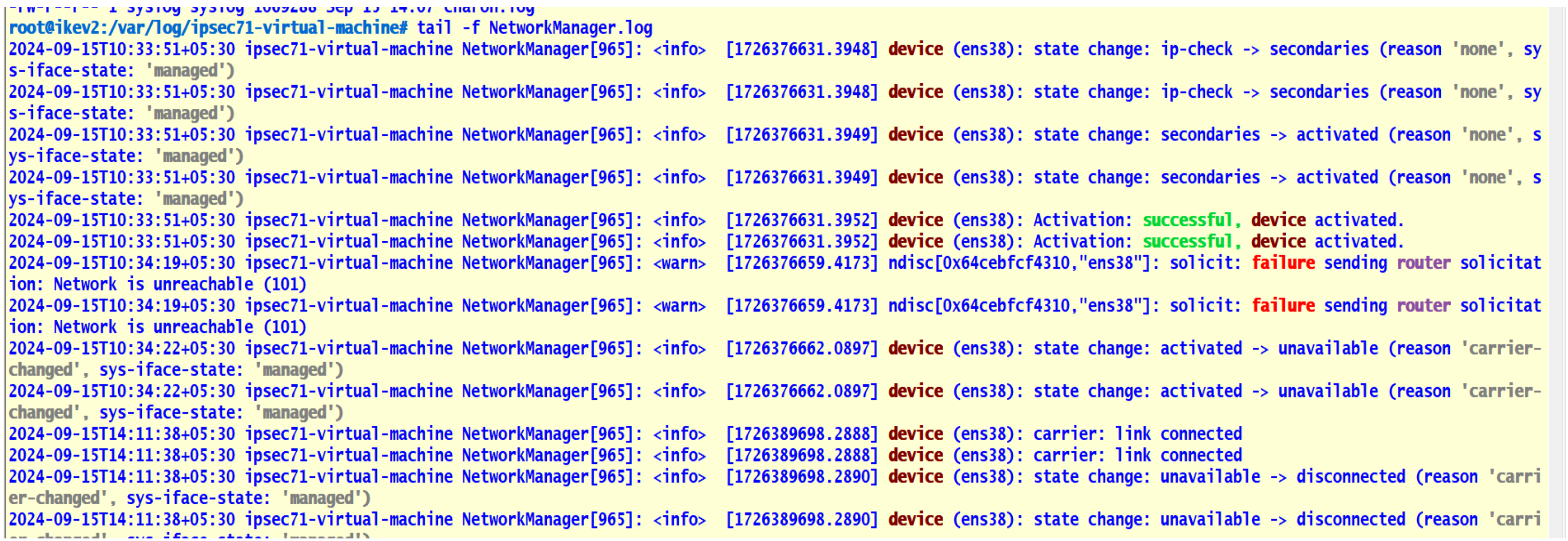
Vaan Megam
Networks

Syslog-DEMO





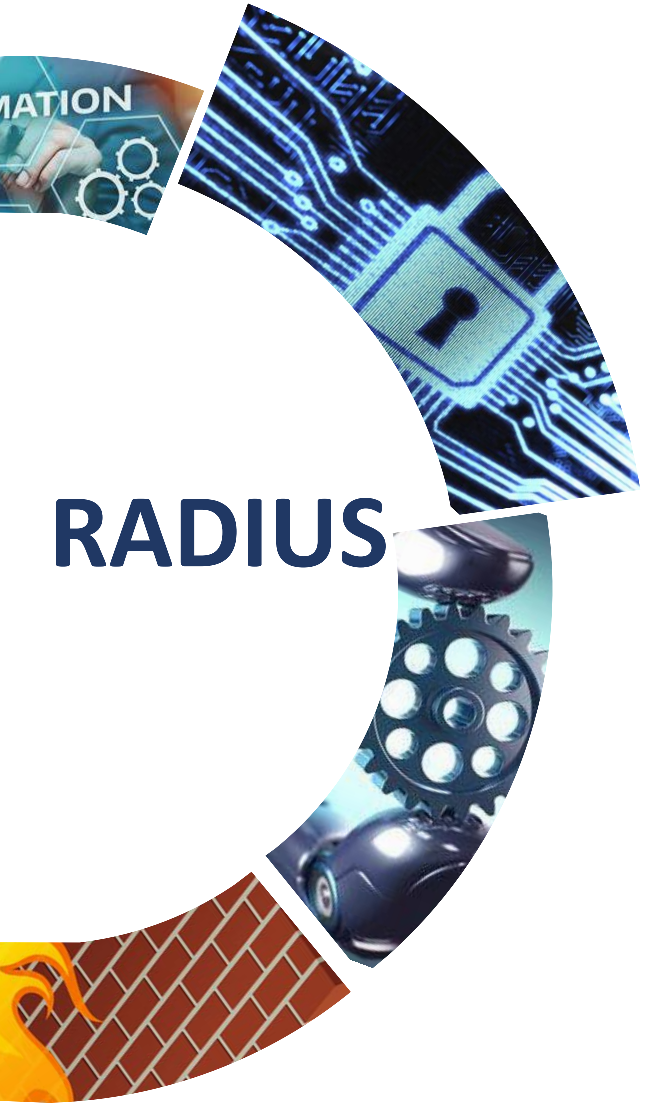
```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

#Limit access to specific subnet, ip host or domain
#
#
$AllowedSender UDP, 127.0.0.1, 192.168.20.0/24
$AllowedSender TCP, 127.0.0.1, 192.168.20.0/24


#Template for recievede remote messages

#
$template remote-incoming-logs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?remote-incoming-logs
```



```
-rw-r--r-- 1 syslog syslog 1009288 Sep 15 14:07 charon.log
root@ikev2:/var/log/ipsec71-virtual-machine# tail -f NetworkManager.log
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3948] device (ens38): state change: ip-check -> secondaries (reason 'none', sy
s-iface-state: 'managed')
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3948] device (ens38): state change: ip-check -> secondaries (reason 'none', sy
s-iface-state: 'managed')
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3949] device (ens38): state change: secondaries -> activated (reason 'none', s
ys-iface-state: 'managed')
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3949] device (ens38): state change: secondaries -> activated (reason 'none', s
ys-iface-state: 'managed')
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3952] device (ens38): Activation: successful, device activated.
2024-09-15T10:33:51+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376631.3952] device (ens38): Activation: successful, device activated.
2024-09-15T10:34:19+05:30 ipsec71-virtual-machine NetworkManager[965]: <warn>  [1726376659.4173] ndisc[0x64cebfcf4310,"ens38"]: solicit: failure sending router solicitat
ion: Network is unreachable (101)
2024-09-15T10:34:19+05:30 ipsec71-virtual-machine NetworkManager[965]: <warn>  [1726376659.4173] ndisc[0x64cebfcf4310,"ens38"]: solicit: failure sending router solicitat
ion: Network is unreachable (101)
2024-09-15T10:34:22+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376662.0897] device (ens38): state change: activated -> unavailable (reason 'carrier-
changed', sys-iface-state: 'managed')
2024-09-15T10:34:22+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726376662.0897] device (ens38): state change: activated -> unavailable (reason 'carrier-
changed', sys-iface-state: 'managed')
2024-09-15T14:11:38+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726389698.2888] device (ens38): carrier: link connected
2024-09-15T14:11:38+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726389698.2888] device (ens38): carrier: link connected
2024-09-15T14:11:38+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726389698.2890] device (ens38): state change: unavailable -> disconnected (reason 'carri
er-changed', sys-iface-state: 'managed')
2024-09-15T14:11:38+05:30 ipsec71-virtual-machine NetworkManager[965]: <info>  [1726389698.2890] device (ens38): state change: unavailable -> disconnected (reason 'carri
er-changed', sys-iface-state: 'managed')
```

Vaan Megam
Networks

RADIUS



RADIUS stands for Remote Authentication Dial-In User Service, is a security protocol used in the AAA framework to provide centralized authentication for users who want to gain access to the network.
It uses UDP port number 1812 for authentication and authorization and 1813 for accounting.

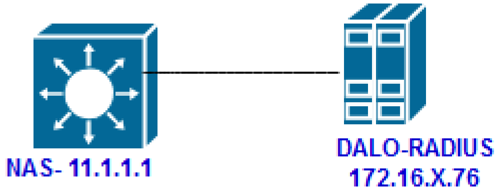
RADIUS enables centralized authentication and authorization, which means that user credentials can be stored in a central database, simplifying network administration and reducing the risk of security breaches.

RADIUS can be integrated with other network protocols, such as LDAP or Kerberos, to provide even greater flexibility and functionality.

- ➢ User sends a request to network access server (NAS)
- ➢ NAS sends access requests to RADIUS server

When the RADIUS server gets the message, it can respond in three different ways: accept access, reject it, or challenge it. When the access request is accepted, access is granted. When the request is rejected, access is not granted, and in the case of a challenge, the RADIUS server requests more information before allowing access

DEMO



```
C3850_CSR_SSR#  show run | section radius
aaa authentication login default group radius local
aaa authorization exec default group radius if-authenticated
aaa accounting exec default start-stop group radius
radius server dalosim
 address ipv4 11.1.1.1 auth-port 1812 acct-port 1813
 key testing123
C3850_CSR_SSR#
```

Radius configs:

Create a new user with Crypto password
Configure the NAS IP with an appropriate type

THANK YOU

Vaan Megam
Networks