Converged Network: Living in a Network Centric World

Intelligent Networks allow handheld devices to receive news, Emails, and to send text.

Video conferencing around the globe is in the palm of your hand.

Phones connect globally to share voice, text and images.

The Human Network is everywhere.

Online gaming connects thousands of people seamlessly.
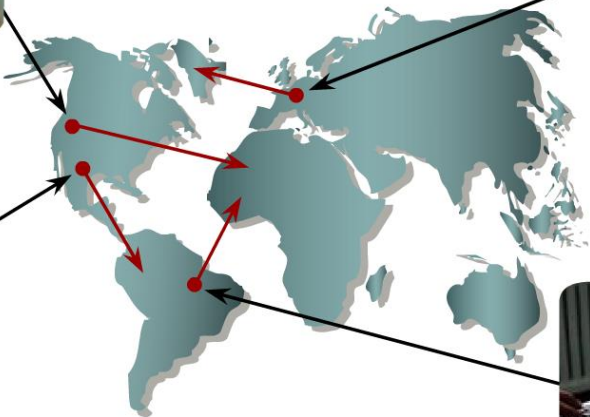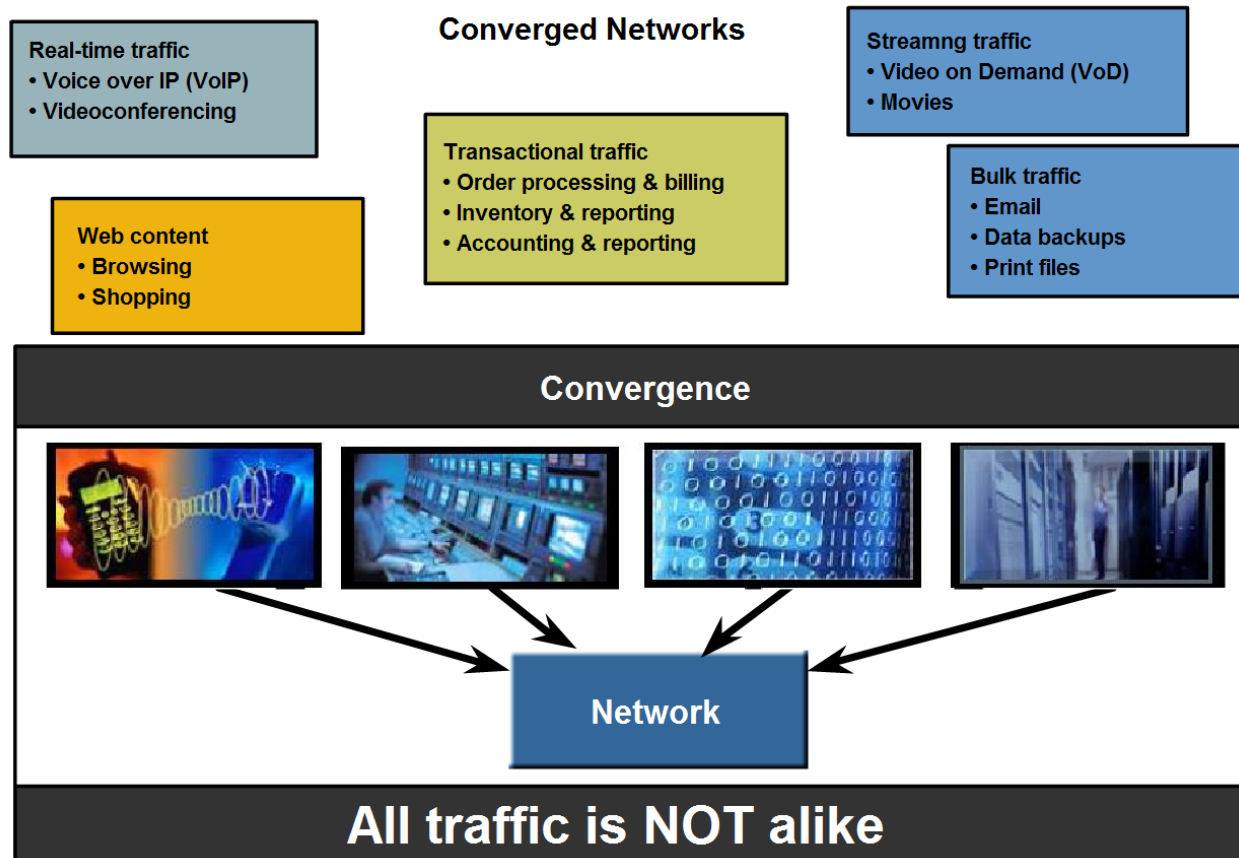
By,

Mr. Kumar Pudashine, (MEng, AIT, Bangkok)
CISA, CISM, CRISC, CNDA, CDCP, COBIT 5, CCNP (Enterprise), JNCIA, CEH v9, ITIL, ISO 27001:2013, AcitivIdentity Certified
Senior Section Chief, Network and Security
Agricultural Development Bank,
Kathmandu

Converged Networks

Intelligent Networks allow handheld devices to receive news, Emails, and to send text.

Phones connect globally to share voice, text and images.

The Human Network is everywhere.

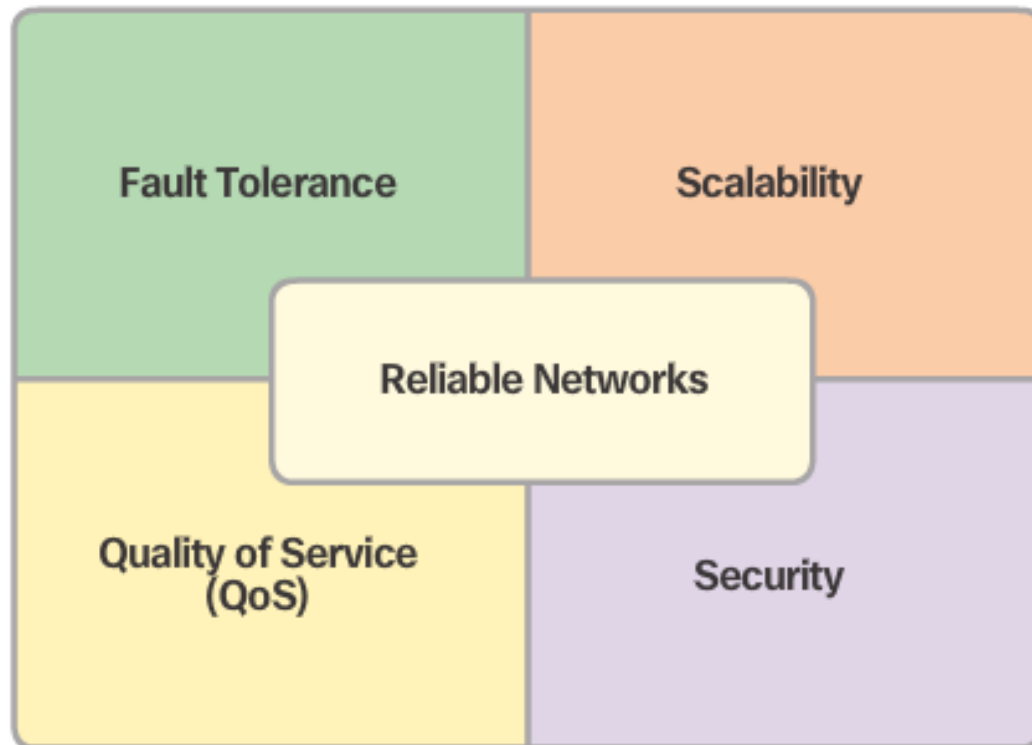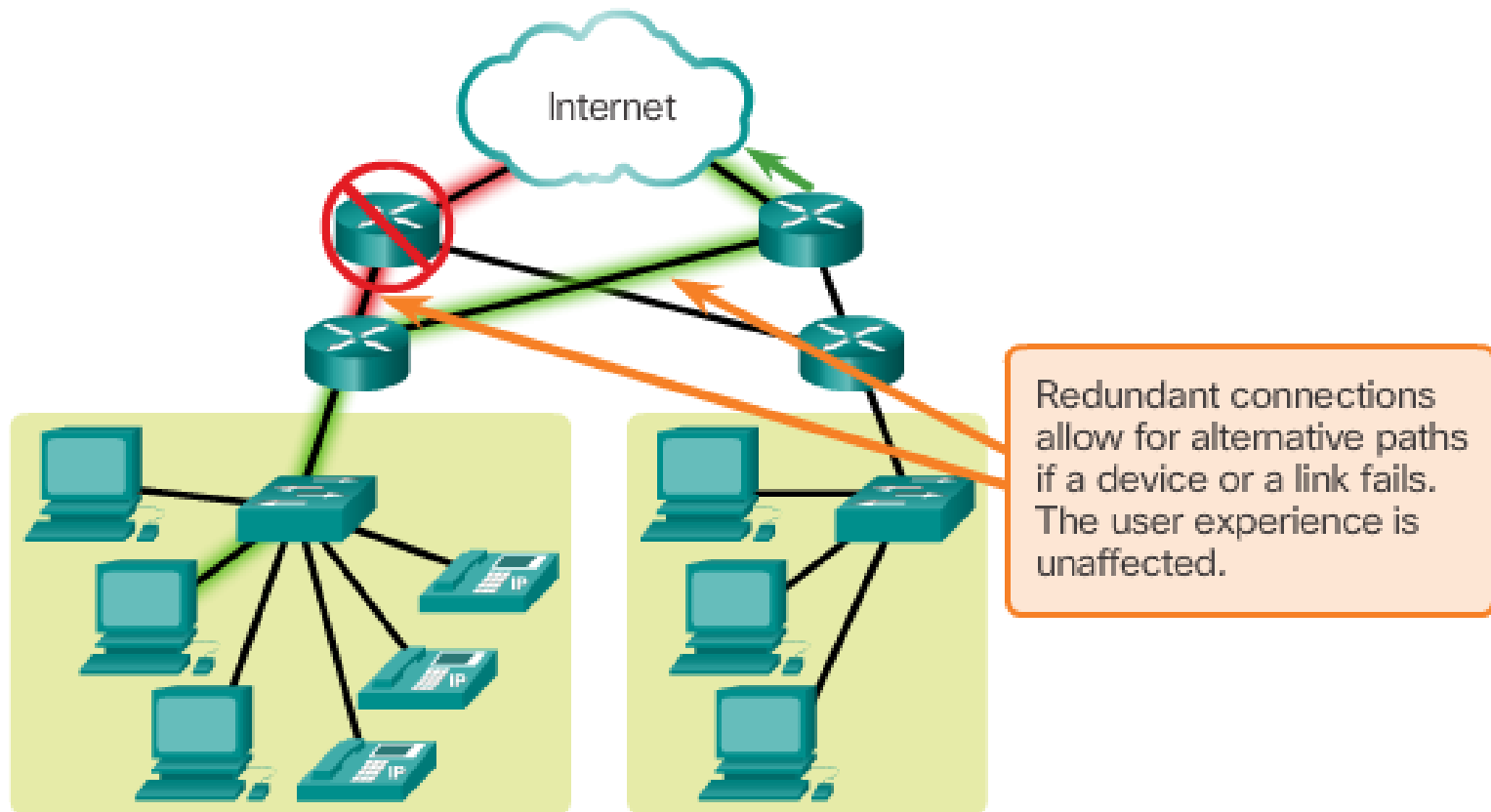Video conferencing around the globe is in the palm of your hand.

Online gaming connects thousands of people seamlessly.

Converged Networks

Reliable Converged Networks

Fault Tolerance

Internet

Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.
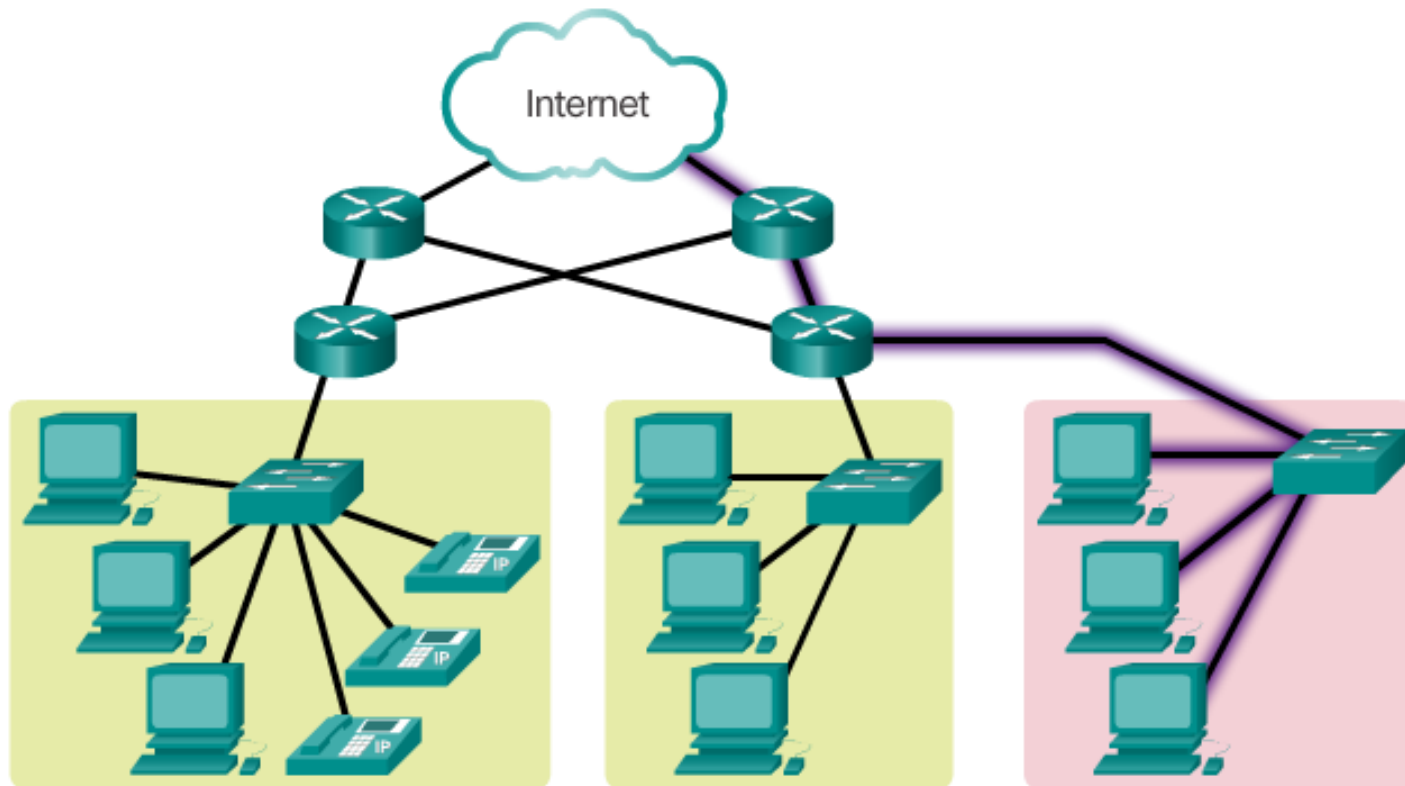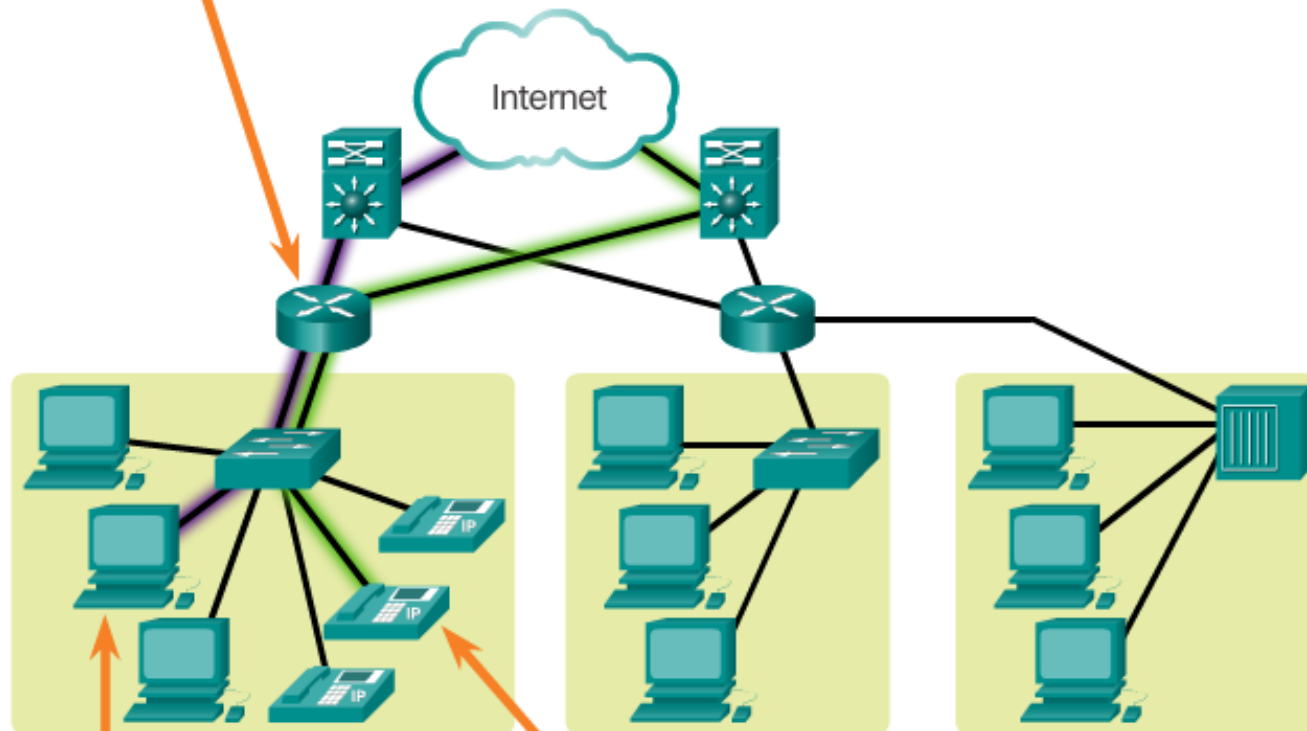
Scalability

Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

Quality of Service

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.
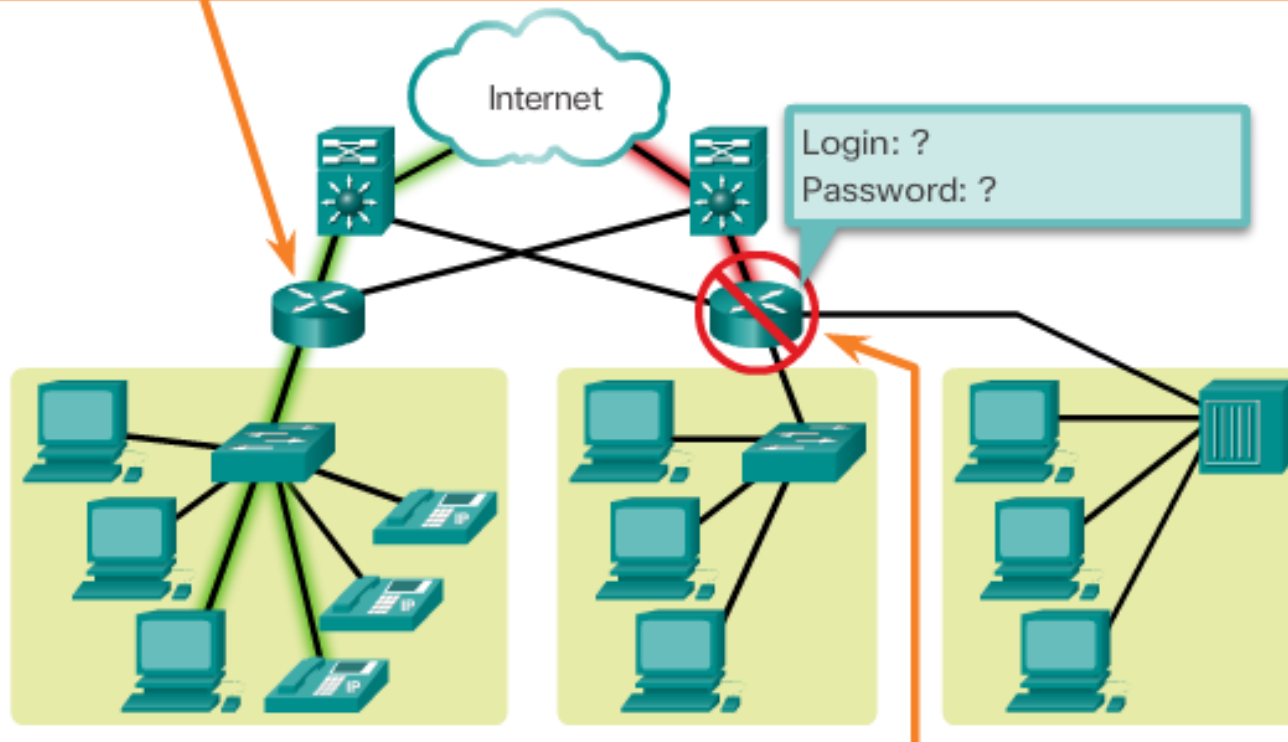
Internet

Web pages can usually receive a lower priority.

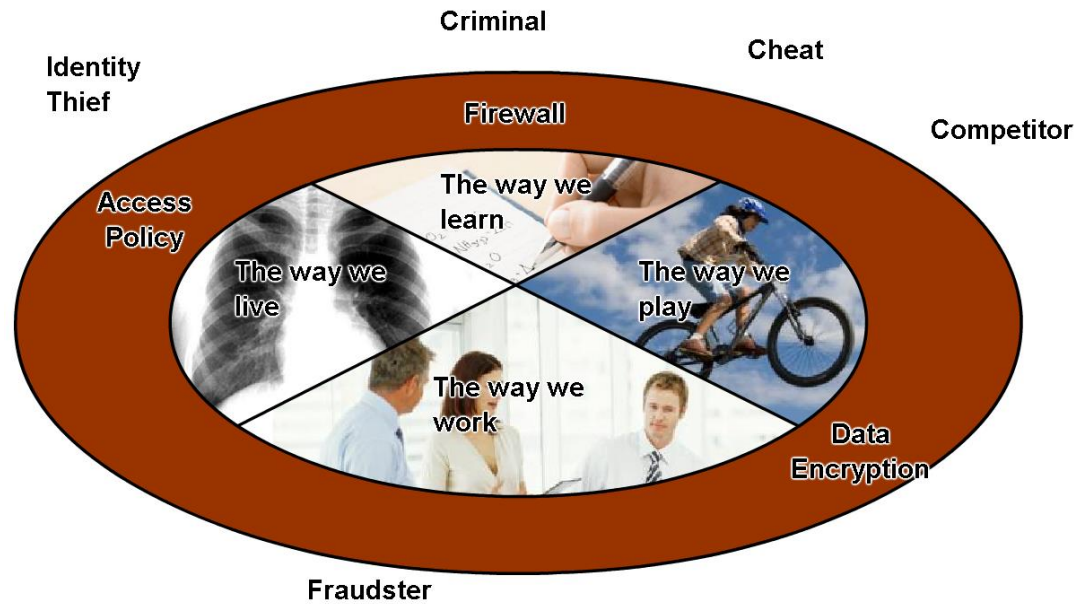Streaming media will need priority to maintain a smooth, uninterrupted user experience.

Security

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.
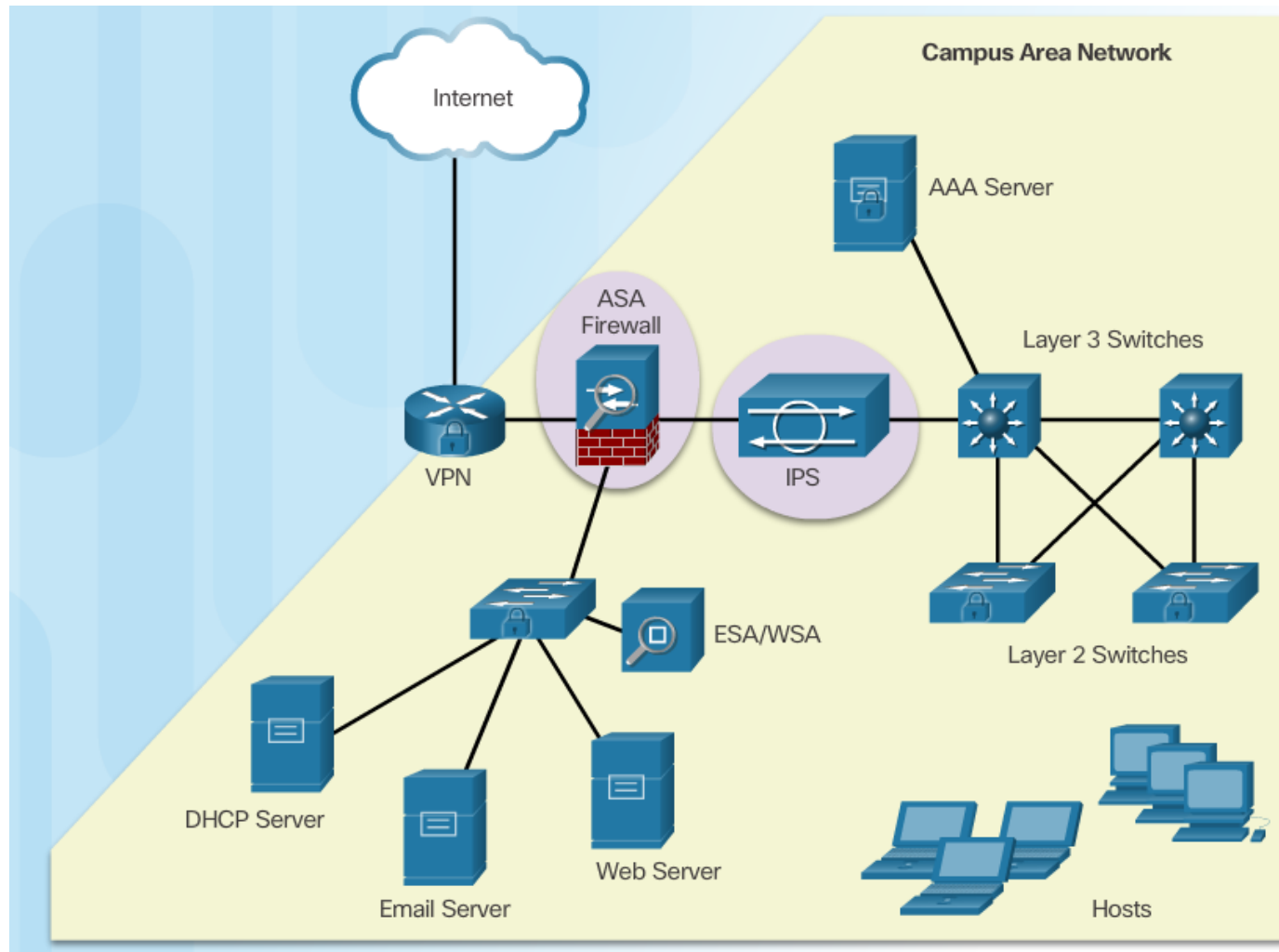
Internet

Login: ?
Password: ?

Security measures protect the network from unauthorized access.
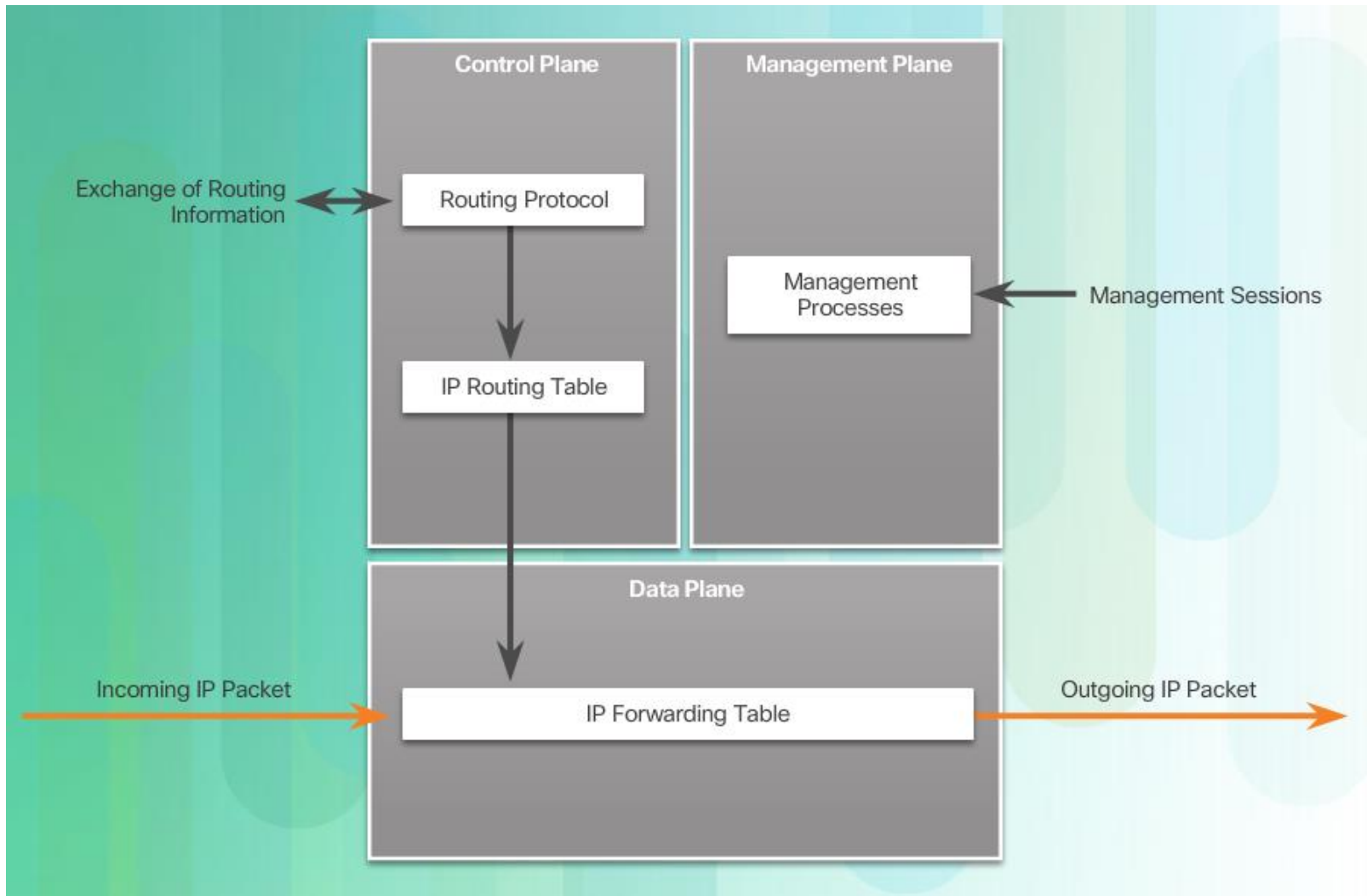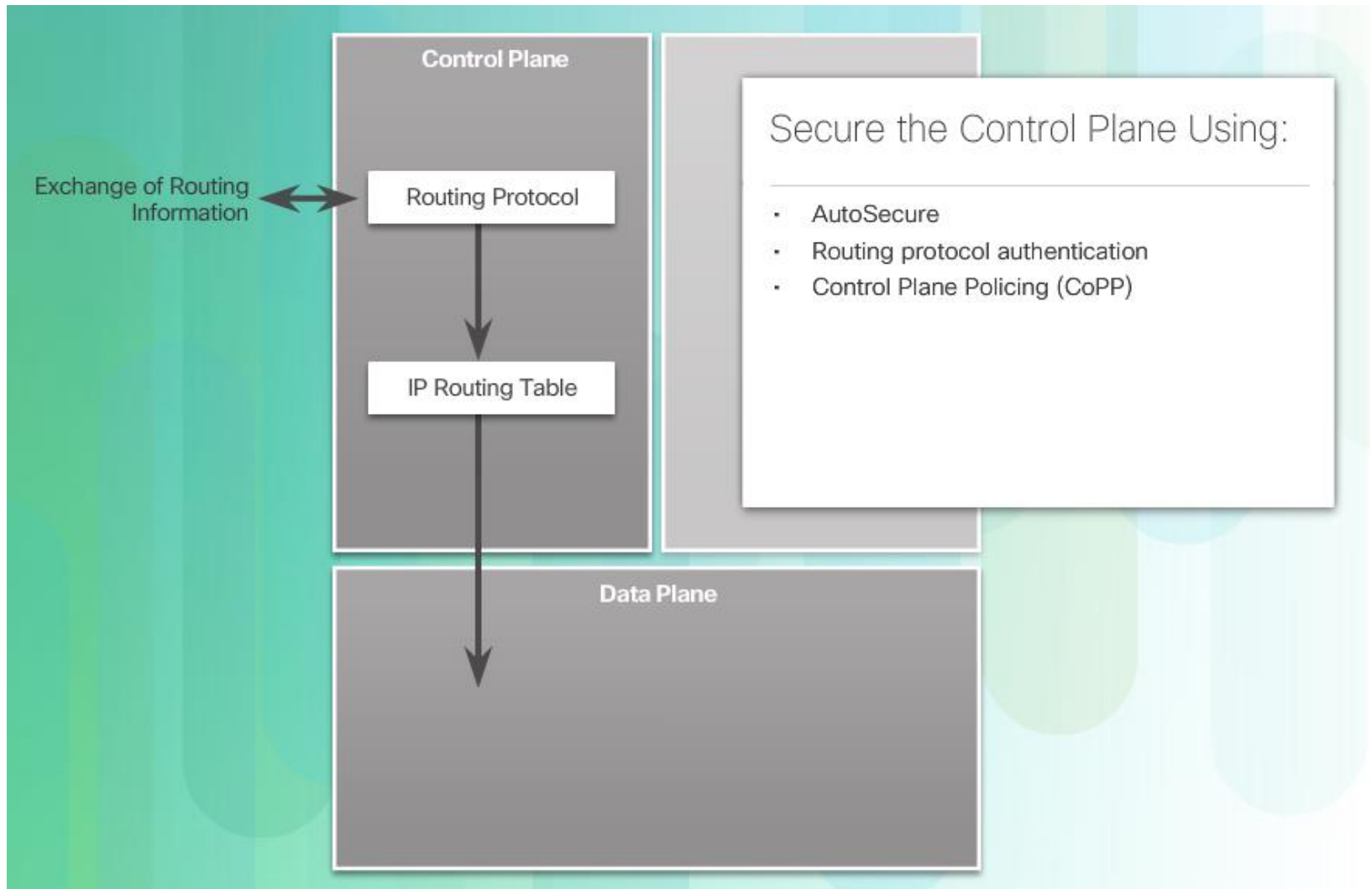
Security

Evolution of Network Security Tools

NFP : Network Foundation Protection Framework

NFP : Securing the Control Plane

NFP : Securing the Management Plane

Secure the Management Plane By:

- Enabling login and password policy
- Presenting legal notification
- Ensuring the confidentiality of data using SSH and HTTPS
- Enabling role-based access control
- Authorizing actions
- Enabling management access reporting

Management Plane

Management Processes

Management Sessions

NFP : Securing the Data Plane

Control Plane

Secure the Data Plane Using:

- ACLs
- Antispoofing
- Layer 2 security including port security, DHCP snooping, dynamic ARP inspection (DAI)

Data Plane

Incoming IP Packet

IP Forwarding Table

Outgoing IP Packet
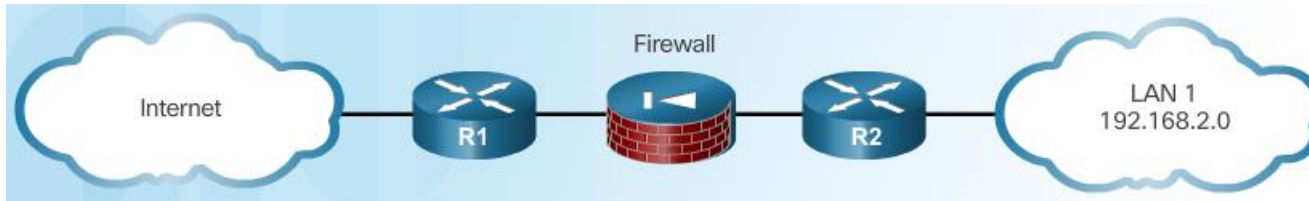
Securing the Network Infrastructure

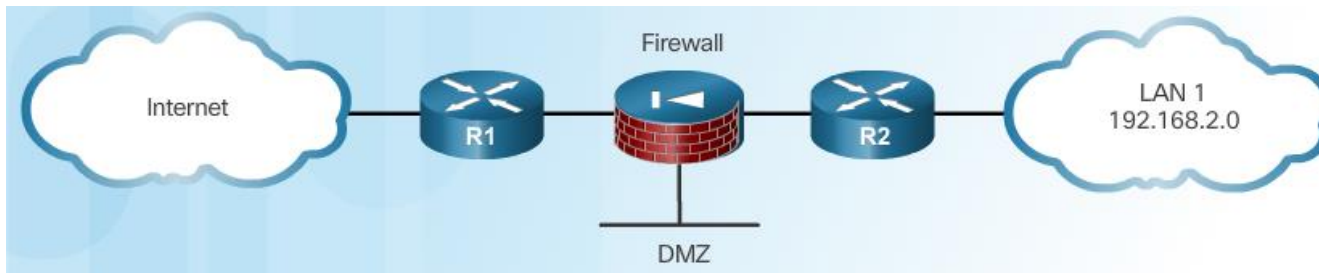# Edge Router Security Approaches

Single Router Approach

Defense in Depth Approach

DMZ Approach

Three Areas of Router Security

Physical Security

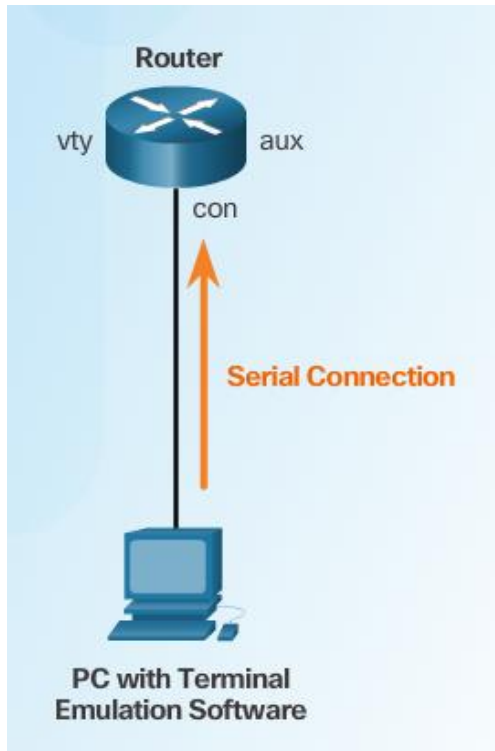Router Operating System and Configuration File Security

Router Hardening
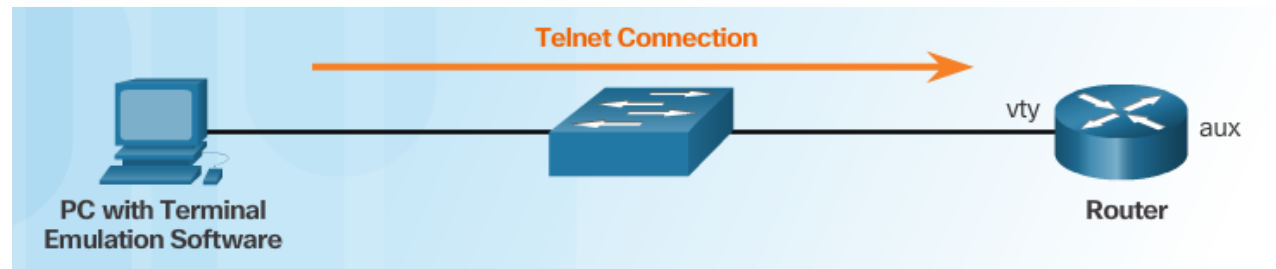
Secure Administrative Access : Tasks ??

- Restrict device accessibility

- Log and account for all access

- Authenticate access

- Authorize actions

- Present legal notification

- Ensure the confidentiality of data
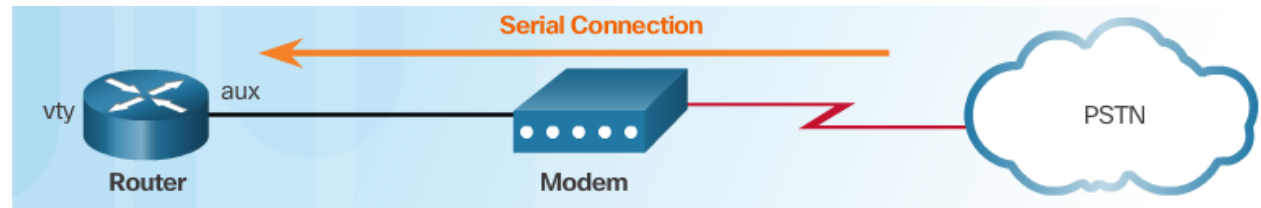
Secure Local and Remote Access

Local Access

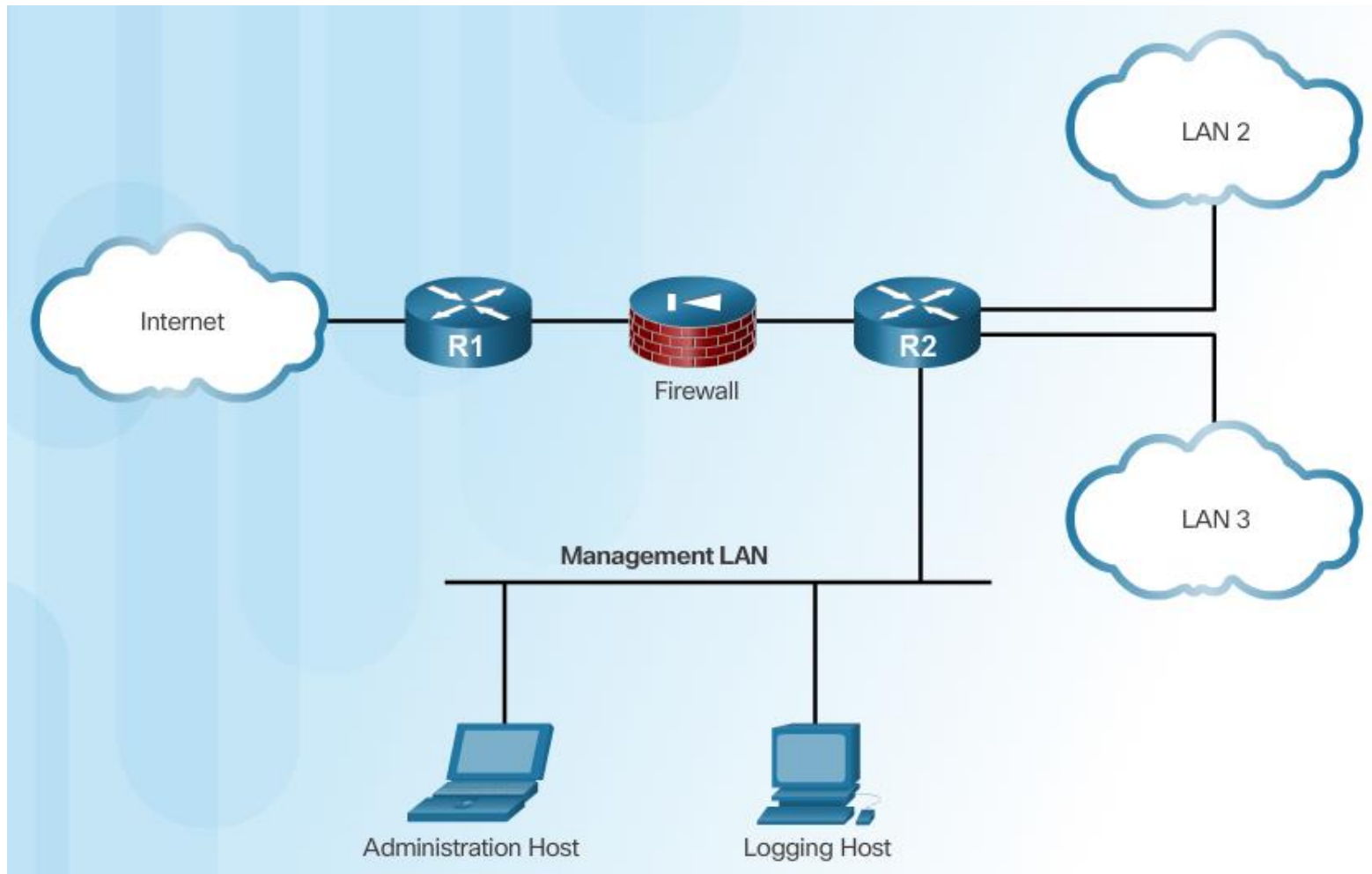## Remote Access Using Telnet

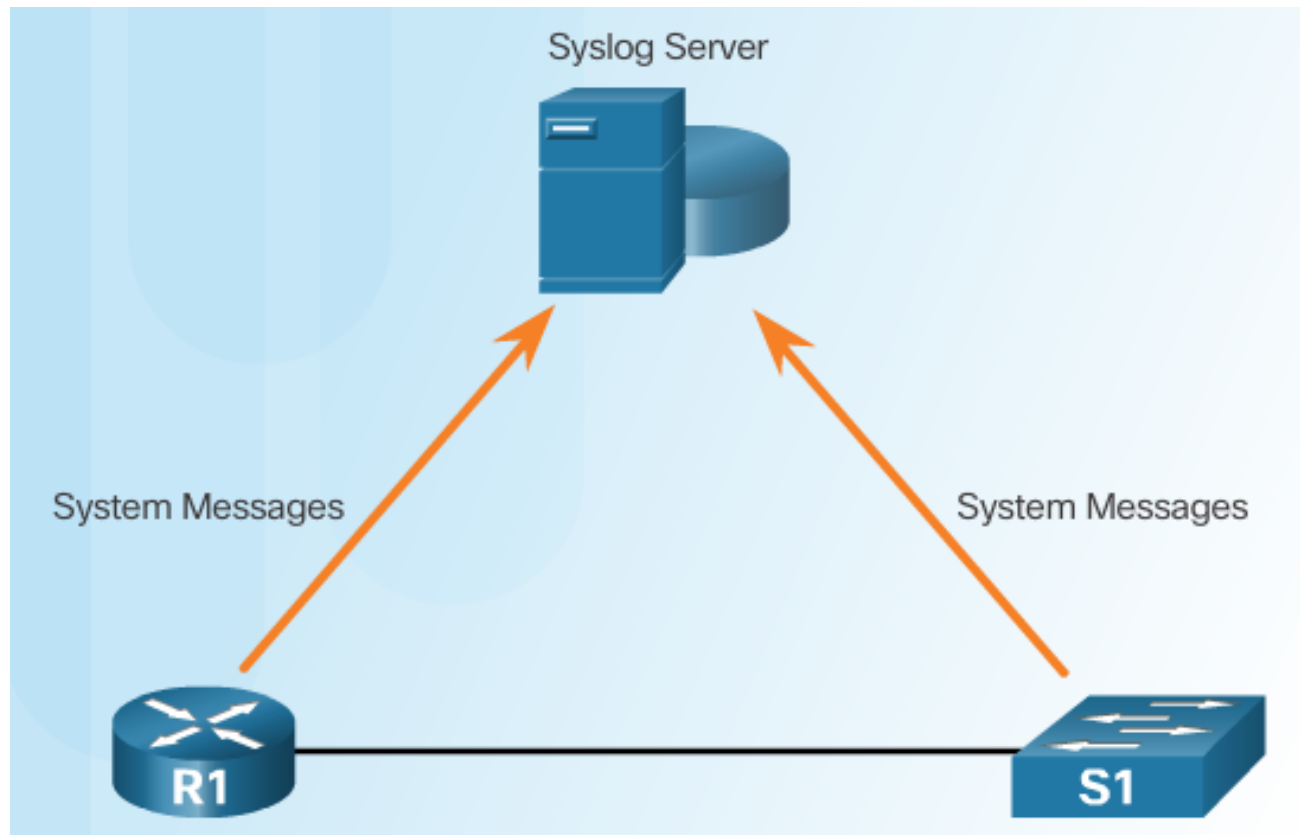## Remote Access Using Modem and Aux Port
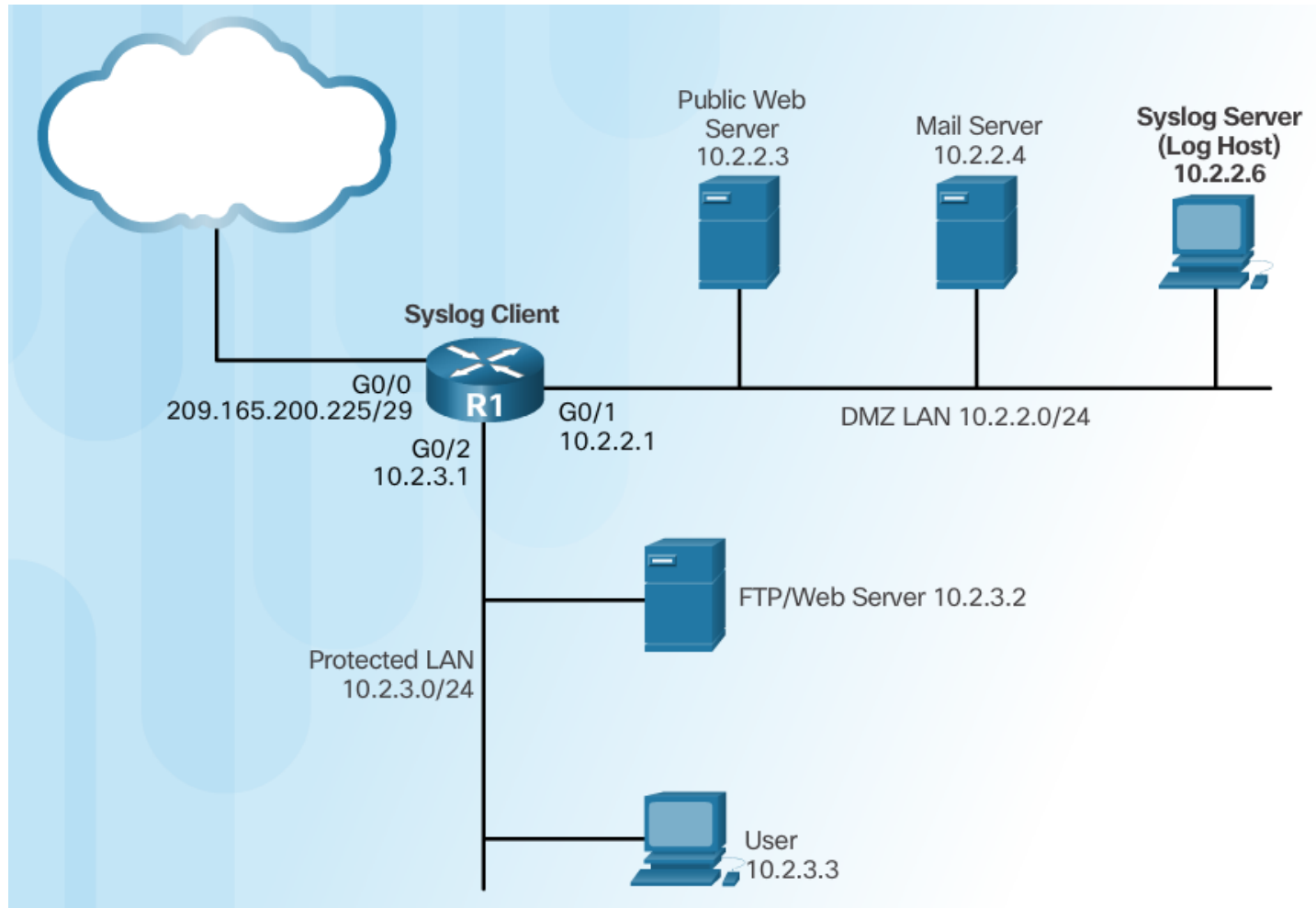
Secure Local and Remote Access

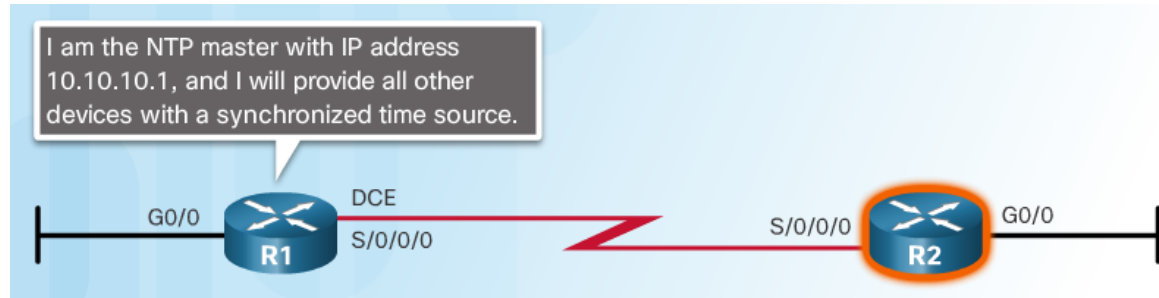Dedicated Management Network

Network Visibility : How To ??

Syslog Systems

NTP Server

Sample NTP Topology

Sample NTP
Configuration on R1

```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```

Sample NTP
Configuration on R2

```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^z
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCF2253E.5DC2A53B (13:01:50.366 UTC Tue Dec 16 2008) clock
offset is 0.3072 msec, root delay is 23.41 msec
root dispersion is 0.38 msec, peer dispersion is 0.05 msec
R2#
```

NTP Authentication


```
R1# conf t
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 cisco123
R1(config)# ntp trusted-key 1
R1(config)# ^z
```

Network Management : FCAPS

1. Performance Management

☐ Quantify, measure, report, analyze and control the performance. (Utilization and Throughput)

2. Fault Management

☐ To log, detect and respond to fault conditions in the network.

3. Configuration Management

☐ To manage configuration of device easily

4. Accounting Management

☐ To enable accounting of user and their policy management.

5. Security Management

☐ To control access to network resources according to defined policy.

Thank You