Build A Small Network

Introduction to Networks v6.0

Chapter 11: Build a Small Network

Pertemuan ke 11 & 12

Kompetensi Khusus

- Mahasiswa mampu mempersiapkan jaringan berskala kecil termasuk rencana pengembangan jumlah perangkat yang memiliki koneksi, mulai dari penentuan topologi jaringan, penentuan perangkat lunak, dokumentasi jaringan, mengelolaan perangkat, pengaturan budget, hingga analisis traffic (C3)

Materi:

1. Network Design
2. Network Security
3. Basic Network Performance
4. Network Troubleshooting

1. Network Design

1.1 Devices in a Small Network

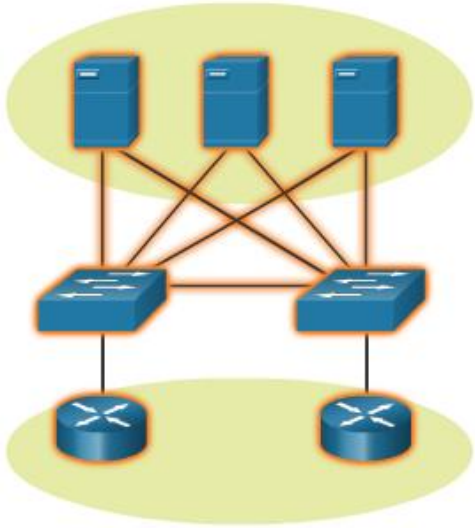
- Small Network Topologies
  - Comprises one router, a couple of switches, and the user PCs.
  - Access to Internet through a single WAN link, cable or DSL.
  - Management usually by a third party company.

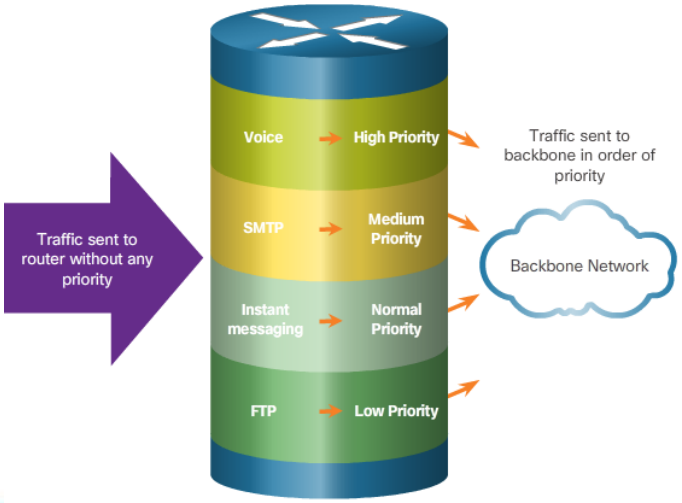
- Device Selection for a Small Network
  - Security, QoS, VoIP, L3 switching, NAT, and DHCP

- IP Addressing for a Small Network
  - Address space is a crucial component of a network design.
  - All devices connected to the network require an address.
  - The address scheme must be planned, documented, and maintained.
  - Address space documentation can be very useful for:
  - troubleshooting and control
  - Address documentation is also very important when controlling resource access.

1.1 Devices in a Small Network

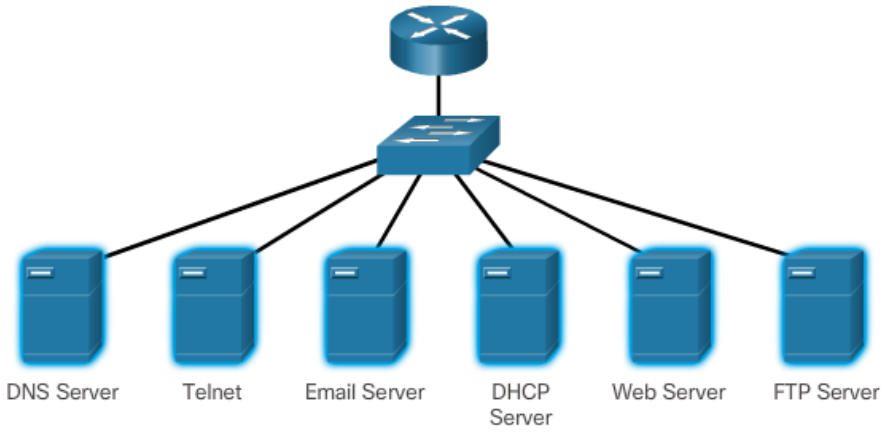
- Redundancy in a Small Network
  - A network should reliable by design.
  - Network failures are usually very costly.
  - Redundancy increases reliability by eliminating single points of failure.
  - Network redundancy can be achieved by duplicating network equipment and links.
  - A good example is a network's link to the Internet or to a server farm.
- Traffic Management
  - Traffic type and patterns are should also be considered when designing a network.
  - A good network design categorizes traffic according to priority.





1.2 Small Network Applications and Protocols

- Common Applications
  - Network Applications
    - Used to communicate over the network.
    - Email clients and web browsers are examples of this type of application.
  - Application Layer Services
    - Programs that interface with the network and prepare the data for transfer.
    - Each service uses protocols, which define the standards and data formats to be used.
- Common Protocols
  - Processes on either end of a communication session
  - How messages are sent and the expected response
  - Types and syntax of messages
  - Meaning of informational fields
  - Interaction with the next lower layer
- Voice and Video Applications
  - Infrastructure
  - VoIP
  - IP Telephony
  - Real-time Applications



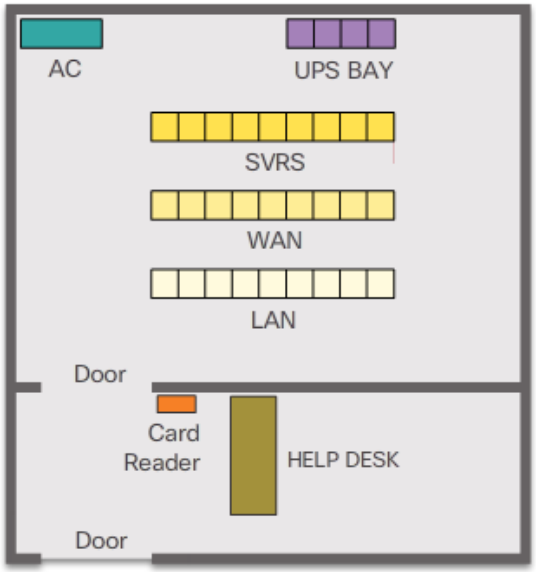
1.3 Scale to Larger Networks

- Small Network Growth
  - To scale a network, several elements are required:
    - Network documentation
    - Device inventory
    - Budget
    - Traffic analysis
- Protocol Analysis
  - Understand the protocols in use in the network.
  - Protocol analyzers are tools designed to help in that task.
  - Capture traffic in high-utilization times and in different locations of the network.
  - Analysis results allow for more efficient way to manage traffic.
- Employee Network Utilization
  - Be aware of how network use is changing.
  - A network administrator can create in-person IT snapshots" of employee application utilization.

2. Network Security

2.1 Security Threats and Vulnerabilities

- Types of Threats
  - Digital intrusion can be costly.
  - Intruders can gain access through software vulnerabilities, hardware attacks, or stolen credentials.
  - Common types of digital threats include those listed in this graphic.
- Physical Security
  - Hardware
  - Environmental
  - Electrical
  - Maintenance
- Types of Vulnerabilities
  - Three primary vulnerabilities: technological, configuration, and security policy
  - Endpoints can be under attack ,such as servers and desktop computers.
  - Any of these three vulnerabilities can be exploited and used in attacks.



Secure computer room floor plan

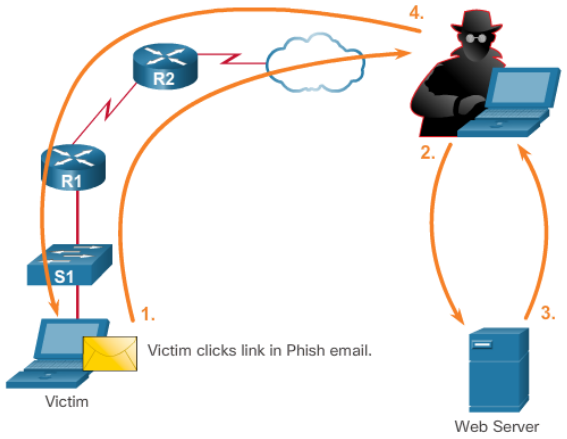
2.2 Network Attacks

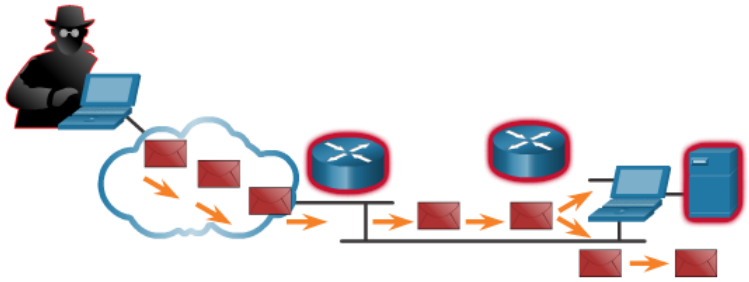
- Types of Malware
  - Viruses
  - Worms
  - Trojan Horses

- Reconnaissance Attacks
  - Discovery and mapping of systems and services
  - Acquire enough information on the target system or network to facilitate the search for vulnerabilities.
  - Common tools rely mostly on free and public Internet services, such as DNS and Whois.
  - Port-scanners and packet sniffers are also commonly used in reconnaissance.

2.2 Network Attacks

- Access Attacks
  - Password Attacks
  - Trust Exploitation
  - Port Redirection
  - Man-in-the-Middle
- Denial of Service Attacks
  - Although simple, DoS attacks are still dangerous.
  - Prevent authorized people from using a service by consuming system resources.
  - Prevent DoS attacks by applying the latest security updates.
  - Common DoS Attacks:
    - Ping of Death
    - SYN Flood
    - DDoS
    - Smurf Attack





2.3 Network Attack Mitigation

- Backup, Upgrade, Update, and Patch
  - Keeping up-to-date with the latest developments
  - Enterprises need to keep current with the latest versions of antivirus software.
  - Patches for all known vulnerabilities must be applied.
  - A central patch server for managing a large number of servers and systems.
  - Patches should be installed without user intervention.
- Authentication, Authorization, and Accounting
  - AAA services provide access control on a network device.
    - Authentication - access a resource
    - Authorization – what they can do
    - Accounting – actions performed while accessing the resource
  - The AAA framework can be very helpful when mitigating network attacks.

2.3 Network Attack Mitigation

- Firewalls
  - A firewall controls the traffic and helps prevent unauthorized access
  - Techniques for determining what is permitted or denied access to a network include:
    - Packet filtering
    - Application filtering
    - URL filtering
    - Stateful packet inspection (SPI)
- Endpoint Security
  - Common endpoints are laptops, desktops, servers, smartphones, and tablets.
  - Securing endpoint devices is challenging.
  - Employees need to be trained on proper use of the network.
  - Policies often include the use of antivirus software and host intrusion prevention.
  - More comprehensive endpoint security solutions rely on network access control.

2.4 Device Security

- Device Security Overview
  - Default settings are dangerous because they are well-known.
  - Cisco routers have the Cisco AutoSecure feature.
  - In addition, the following apply for most systems:
    - Change default usernames and passwords immediately
    - Restrict access to system resources to authorized individuals only.
    - Turn off unnecessary services.
    - Update any software and install any security patches prior to production operation.
- Passwords
  - Use strong passwords. A strong password has/is:
    - At least 8 characters, preferably 10 or more
    - A mix of uppercase and lowercase letters, numbers, symbols, and spaces.
    - No repetition, no common dictionary words, no letter or number sequences, no usernames, relative, or pet names, and no other easily identifiable pieces of information
    - Misspelled words
    - Changed often
  - Cisco routers support the use of a phrase made of many words, which is called a passphrase.

2.4 Device Security

- Basic Security Practices
  - Strong passwords are only as useful as they are secret.
  - The **service password-encryption** command encrypts the passwords in the configuration.
  - The **security passwords min-length** command ensures all configured passwords have a minimum specified length.
  - Blocking several consecutive login attempts helps minimize password brute-force attacks.
  - **login block-for 120 attempts 3 within 60** will block login attempts for 120 seconds if there are three failed login attempts within 60 seconds.
  - **exec timeout** automatically disconnect idle users on a line
- Enable SSH
  - Telnet is not secure.
  - It is highly recommended to use SSH for remote shell protocol.
  - To configure a Cisco device to support SSH takes four steps:

  Step 1. Ensure that the router has a unique hostname and a IP domain name.

  Step 2. Generate the SSH keys.

  Step 3. Create a local username.

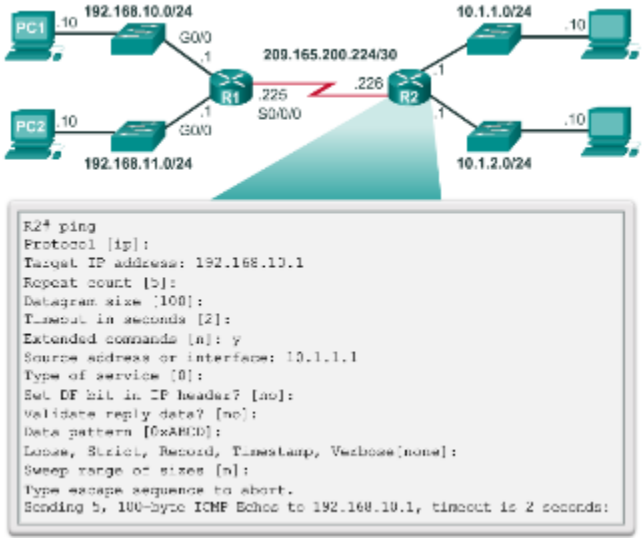
  Step 4. Enable vty inbound SSH sessions.
  - The router can now be remotely accessed only by using SSH.

3. Basic Network Performance

3.1 The ping Command

- Interpreting Ping Results
  - Using the ping command is an effective way to test connectivity.
  - Use the Internet Control Message Protocol (ICMP) to verify Layer 3 connectivity.
  - Help to identify the source of the problem.
  - What do these common ping indicators tell you?

    ! . U
  - Extended Ping
    - Allows for more options
- Network Baseline
  - Built over a period of time.
  - Saved results from commands, such as ping or trace, along with error messages an response times
  - Time stamped for later comparison.
  - Increased response time could indicate latency issue.



3.2 The traceroute and tracert Command

- Interpreting Trace Message
  - Returns a list of hops as a packet is routed through a network.
  - Use tracert for Windows-based systems.
  - Use traceroute for Cisco IOS and UNIX-based systems.
- Extended Traceroute
  - Allows adjustment of parameters
  - Command terminates when:
    - Destination responds with an ICMP echo reply
    - User interrupts the trace with the escape sequence

```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
1 2 ms 2 ms 2 ms 10.0.0.254
2 * * * Request timed out.
3 * * * Request timed out.
4 ^C
C:\>
```

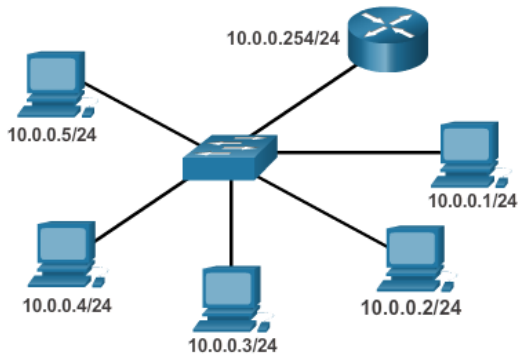
3.3 Show Commands

- The Cisco IOS CLI show commands are powerful troubleshoot tools.
- The show commands display configuration files, checking the status of device interfaces and processes, and verifying the device operational status.
- The status of nearly every process or function of the router can be displayed using a show command.
- Some of the more popular show commands are:
  - show running-config
  - show interfaces
  - show arp
  - show ip route
  - show protocols
  - show version

```
R1# show running-config
<Output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
 description LAN 192.168.1.0 default gateway
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

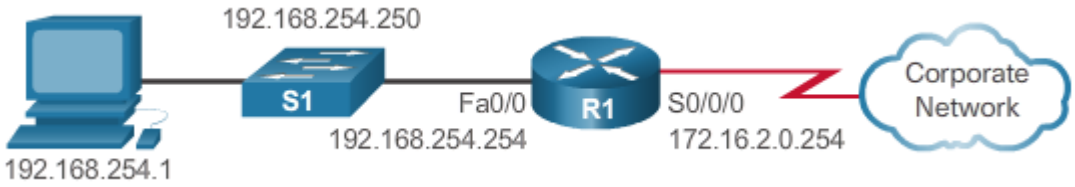
3.4 Host and IOS Commands

- The ipconfig Command
  - Display IP and default gateway information on a Windows-based computer.
  - What do these commands display?
    - ipconfig /all
    - ipconfig /displaydns
- The arp Command
  - The arp –a command lists all devices currently in the ARP cache of the host.
  - The cache can be cleared by using the arp -d command.



3.4 Host and IOS Commands

- The show cdp neighbors Command
  - CDP is a Cisco-proprietary protocol that runs at the data link layer.
  - Two or more Cisco network devices can learn about each other even if Layer 3 connectivity does not exist.
  - CDP can be a security risk.
  - To disable CDP globally, use the global configuration command no cdp run.
  - To disable CDP on an interface, use the interface command no cdp enable.
  - What information does the cdp neighbors details command provide?
- The show ip interface brief Command
  - Displays a summary of the key information for all the network interfaces on a router.
  - Verify the status of the switch interfaces.



3.5 Debugging

- The debug Command
  - Allows the administrator to display messages generated by the following processes in real-time for analysis:
    - IOS processes
    - Protocols
    - Mechanisms
    - Events
  - **undebug all** turns off all debug commands
  - What are the available debug commands?
  - What can you do to limit the amount of displayed messages?
- The terminal monitor Command
  - Displays the log messages while connected remotely, such as SSH
  - Stop displaying the log message: **terminal no monitor**

```
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1# undebug all
All possible debugging has been turned off
R1#
```

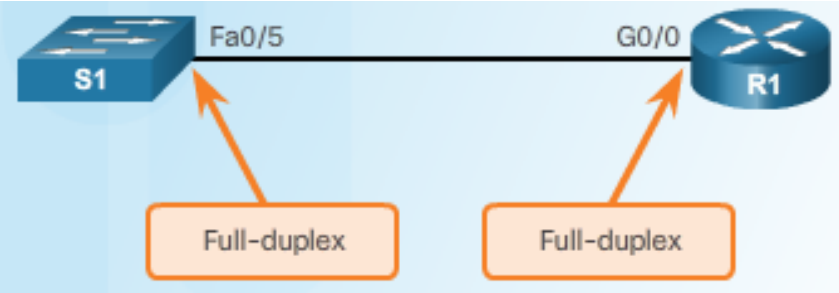
4. Network Troubleshooting

4.1 Troubleshooting Methodologies

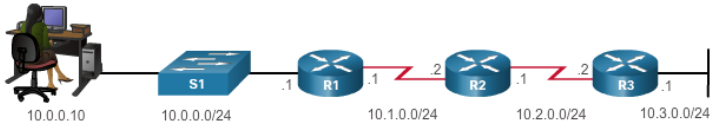
- Basic Troubleshooting Approaches
  - Identify the Problem
  - Establish a Theory of Probable Causes
  - Test the Theory to Determine Cause
  - Establish a Plan of Action to Resolve the Problem and Implement the Solution
  - Verify Full System Functionality and Implement Preventative Measures
  - Document Findings, Actions, and Outcomes
- Resolve or Escalate?
- Verify and Monitor Solution
  - What IOS commands can you use to verify and monitor the solution?

4.2 Troubleshoot Cables and Interfaces

- Duplex Operation
  - Direction of data transmission between two devices
  - Two connected Ethernet network interfaces should operate in the same duplex mode for best performance
- Duplex Mismatch
  - Log messages can indicate duplex mismatches.
  - What IOS commands can you use to determine duplex mismatch?



4.3 Troubleshooting Scenarios



- IP Addressing Issues on IOS Devices
  - Manual assignment mistakes
  - DHCP-related issues
  - Which show commands?
- IP Addressing Issues on End Devices
  - 169.254.0.0/16 on Windows-based system
  - ipconfig to verify IP addresses assigned to a Windows-based system

```
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd4c:6609:6733:c5cc%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

C:\>
```

- Default Gateway Issues
  - Unable to communicate outside the network
  - **ipconfig** to verify default gateway assigned to a Windows-based system
- Troubleshooting DNS Issues
  - **ipconfig /all** to determine DNS server used
  - **nslookup** to manually place DNS queries and analyze DNS response

Chapter Summary

Summary

- Explain how a small network can scale into a larger network.
- Configure switches and routers with device hardening features to enhance security.
- Use common show commands and utilities to establish a relative performance baseline for the network.
- Apply troubleshooting methodologies and command host and IOS commands to resolve problems.
- Explain how a small network of directly connected segments is created, configured, and verifies.

TERIMA KASIH