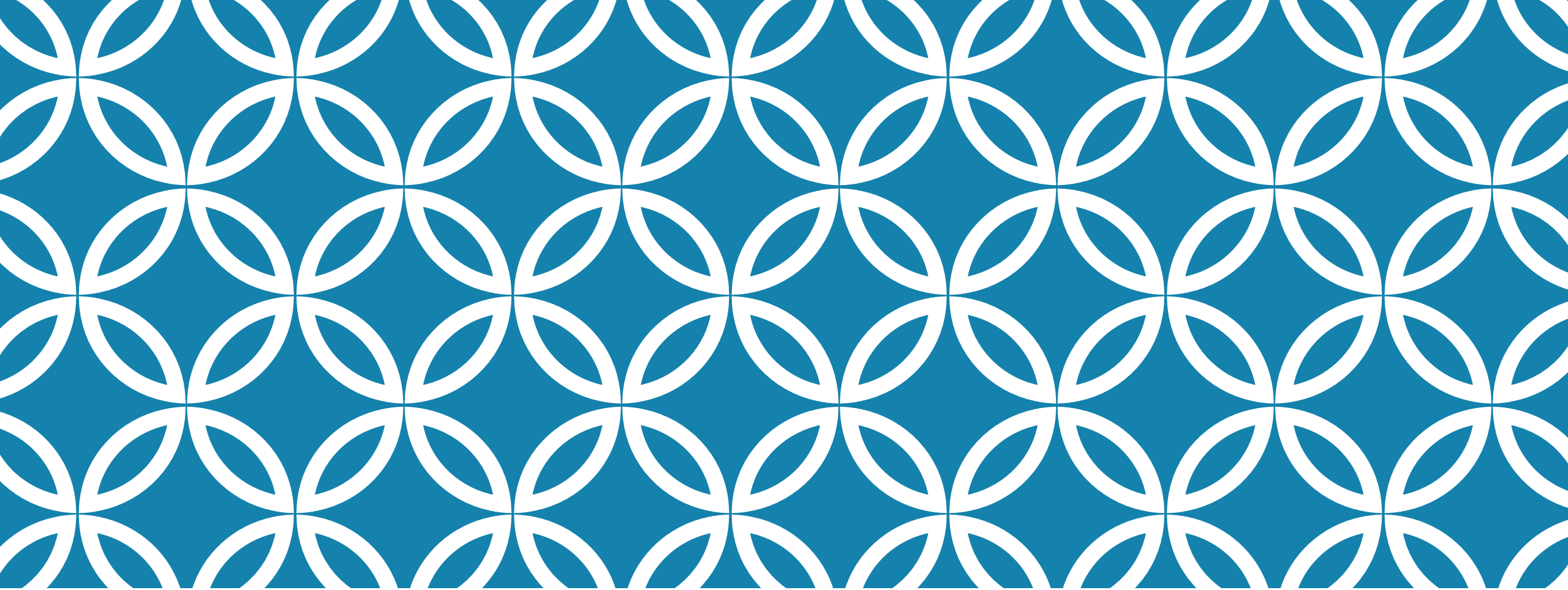


ACCESS CONTROL LIST

Jaringan Komputer 2

SUB CPMK :

MAMPU MENJELASKAN KONSEP ACCESS CONTROL LIST DAN PENERAPANNYA, MENERAPKAN KONSEP NETWORK TRAFFIC SHAPING DAN MAMPU MEMBANDINGKAN KONSEP PEMBUATAN PROXY DAN TRANSPARENT PROXY YANG BERTINGKAT. [C5,A3]

INDIKATOR :

Ketepatan membedakan Tipe ACL, menjelaskan jenis trafik dan mampu menggunakan wildcard masking pada ACL

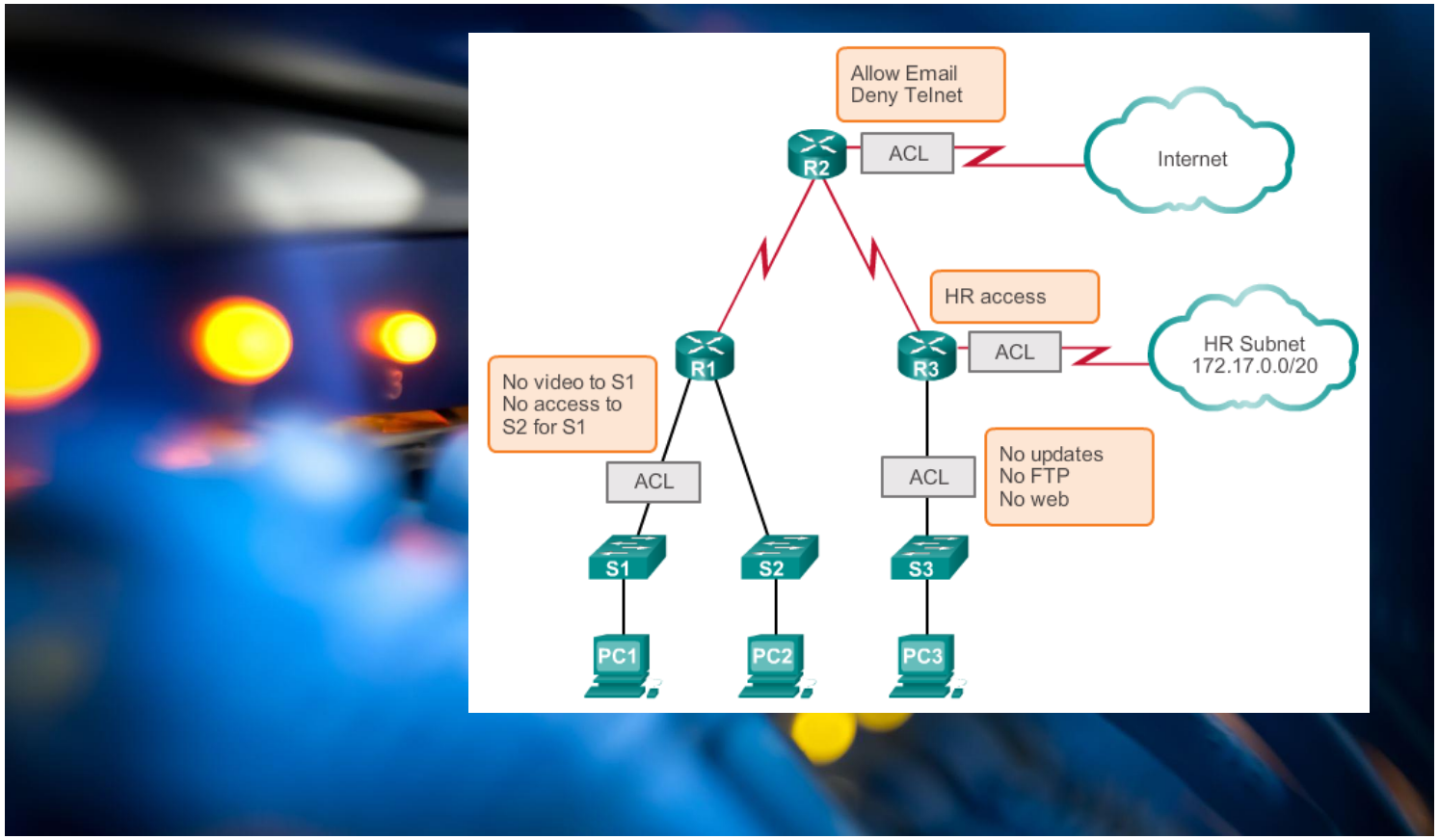
1. Access Control List (ACL)
2. Fungsi ACL
3. Cara Kerja ACL
4. Jenis ACL
5. Jenis Trafik ACL
6. Penerapan ACL

POKOK BAHASAN

OVERVIEW ACL

Access Control List (ACL) adalah tabel yang memberitahu sistem operasi komputer, hak akses apa saja yang dimiliki setiap user ke suatu objek tertentu dari sebuah system. Misalnya berupa direktori, file atau layanan protokol yang lain.

Setiap objek memiliki atribut keamanan sendiri-sendiri yang menentukan siapa yang boleh mengkases sesuai daftar kontrol aksesnya dan siap saja yang ditolak. Daftar tersebut berisi entri untuk setiap hak akses user pada sebuah system.



FUNGSI ACL

Penggunaan access control list yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan sebuah aturan berkenaan dengan system keamanan.

CARA KERJA ACL

Membuat access list sangat mirip dengan statement pada programming **if–then** jika sebuah kondisi terpenuhi maka aksi yang diberikan akan dijalankan, jika tidak terpenuhi, tidak ada yang terjadi dan statemen berikut nya akan dievaluasi

Ketika paket dibandingkan dengan ACL, terdapat beberapa peraturan(rule) penting yang diikuti:

1. Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan, sebagai contoh paket dibandingkan dengan baris pertama dari ACL, kemudian baris kedua, ketiga, dan seterusnya.
2. Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan. Ketika paket cocok dengan kondisi pada baris ACL, paket akan ditindaklanjuti dan tidak ada lagi kelanjutan perbandingan.
3. Terdapat statement “tolak” yang tersembunyi(impilicit deny) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak

JENIS ACL (1)

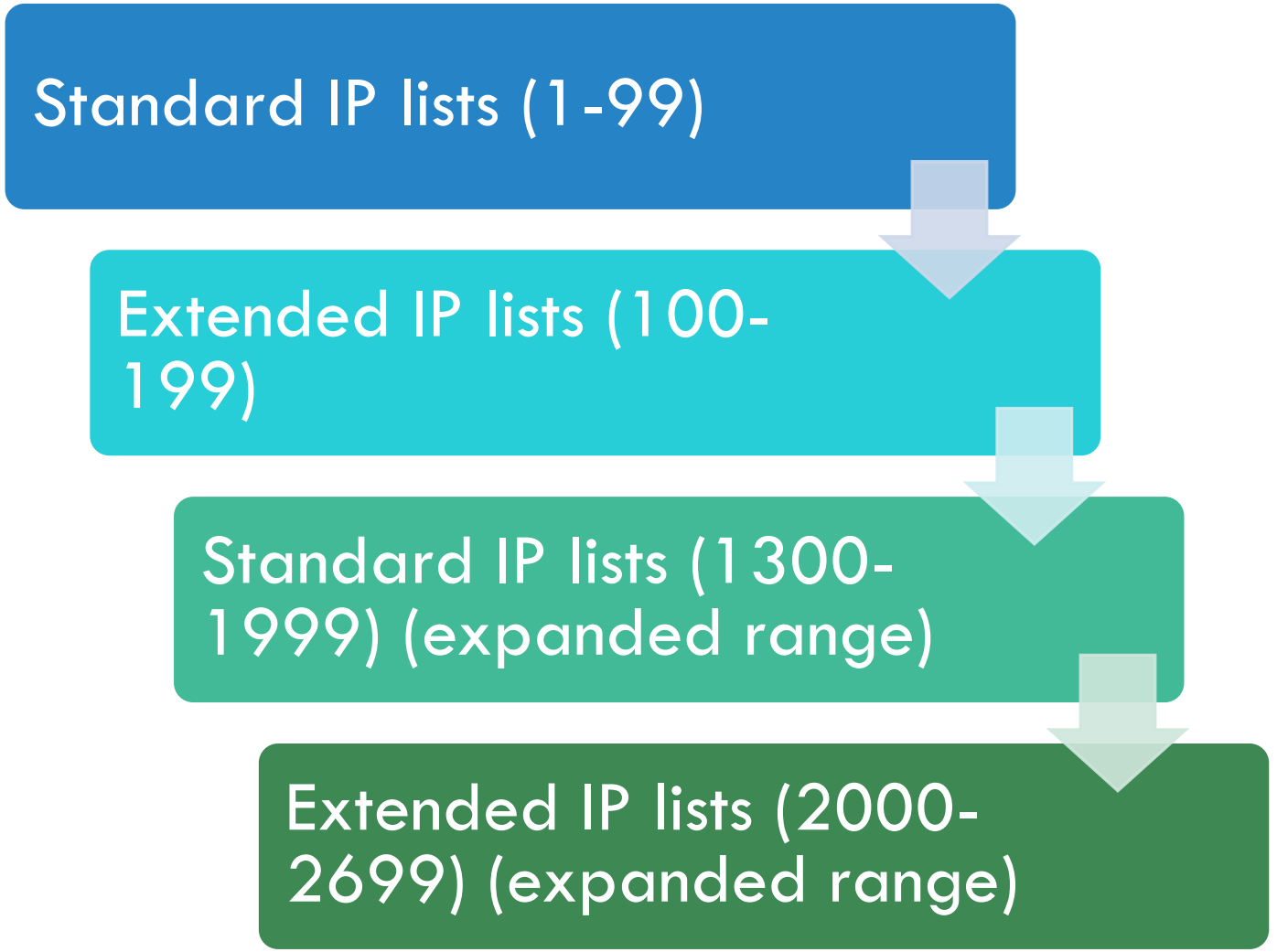
Standard ACL

- hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

Extended ACL

- Bisa mengevaluasi banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, field protocol pada header network layer dan nomor port pada header transport layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas

JENIS ACL (2)


Standard IP lists (1-99)
Extended IP lists (100-199)
Standard IP lists (1300-1999) (expanded range)
Extended IP lists (2000-2699) (expanded range)

Types of Cisco IPv4 ACLs

Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

Types of Cisco IPv4 ACLs

Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

JENIS TRAFIK ACL

Inbound

- Ketika sebuah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.

Outbound

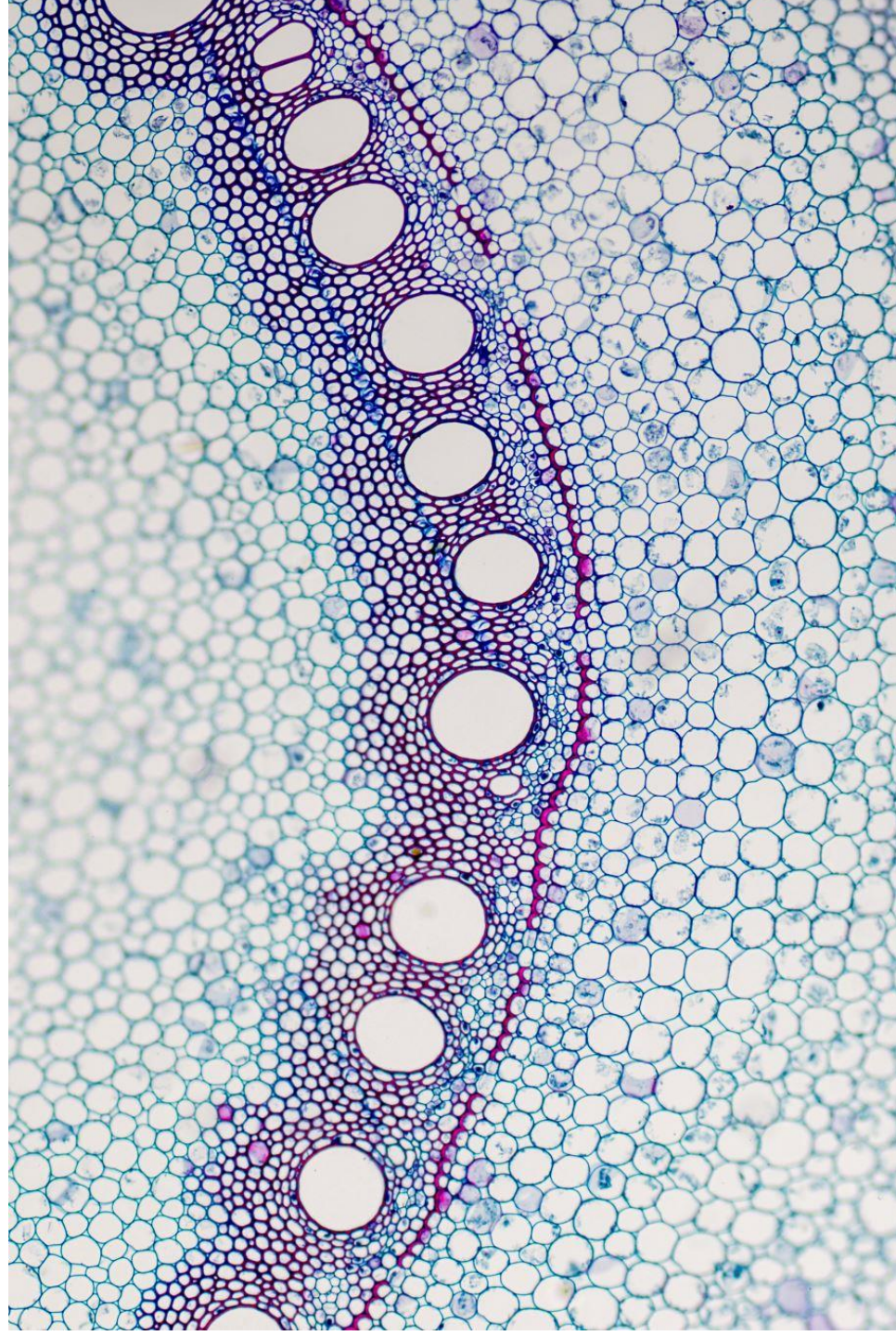
- Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses melalui ACL malalui antrian

PANDUAN UMUM ACL

1. Hanya bisa menerapkan satu ACL untuk setiap interface, setiap protocol dan setiap arah. Artinya bahwa ketika membuat ACL IP, hanya bisa membuat sebuah inbound ACL dan satu Outbound ACL untuk setiap interface.
2. Organisasikan ACL sehingga test yang lebih spesifik diletakkan pada bagian atas ACL
3. Setiap kali terjadi penambahan entry baru pada ACL, entry tersebut akan diletakkan pada bagian bawah ACL. Sangat disarankan menggunakan text editor dalam menggunakan ACL
4. Tidak bisa membuang satu baris dari ACL. Jika kita mencoba demikian, kita akan membuang seluruh ACL. Sangat baik untuk mengcopy ACL ke text editor sebelum mencoba mengubah list tersebut.

WILDCARD MASKING

- ✓ Wildcard masking digunakan Bersama ACL untuk menentukan host tunggal, sebuah **jaringan** atau **range tertentu** dari **sebuah atau banyak network**
- ✓ Untuk menentukan bahwa sebuah oktet bisa bernilai apa saja, angka yang digunakan adalah 255.
- ✓ Sebagai contoh, berikut ini adalah subnet /24 dispesifikasikan dengan wildcard: 172.16.30.0 0.0.0.255 ini memberitahukan pada router untuk menentukan 3 oktet secara tepat, tapi oktet ke-4 bisa bernilai apa saja.

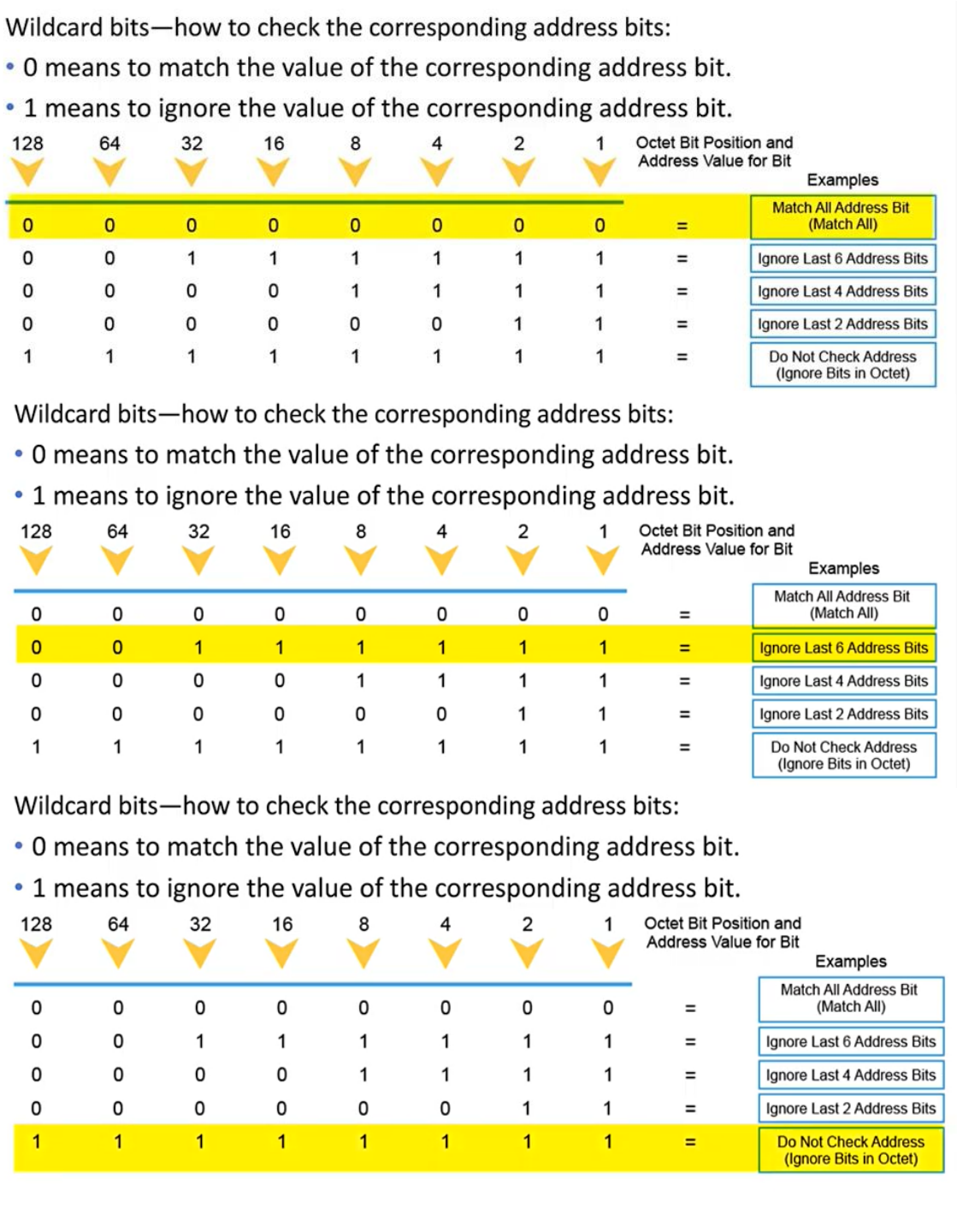


CARA KERJA WILDCARD MASK

Wilcard mask dan subnet mask berbeda penggunaan untuk penerapan kecocokan antara binary 1 dan 0. penggunaan binary 1 dan 0 pada wildcard mask digunakan atauran sebagai berikut :

Wildcard mask bit 0 : harus cocok/sesuai dengan nilai alamat

Wildcard mask bit 1 : diabaikan untuk nilai alamat berapapun



GUIDELINES FOR ACL CREATION

GENERAL GUIDELINES FOR CREATING ACLS (CONT.)

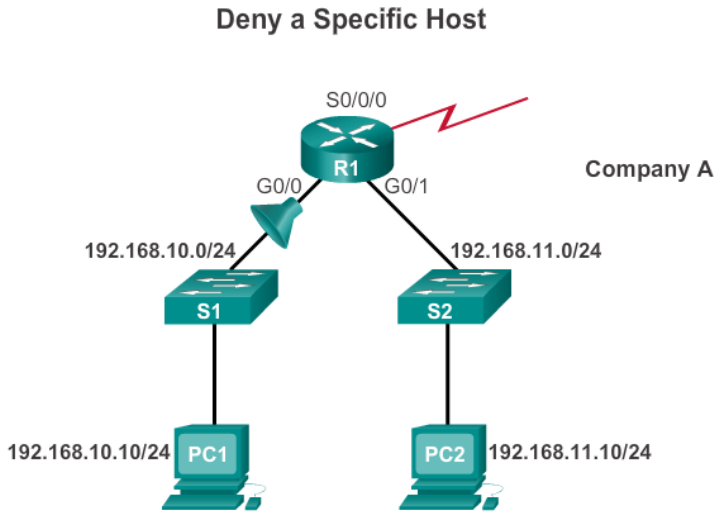
The Three Ps

Satu ACL per protokol - Untuk mengontrol arus lalu lintas pada suatu interface, ACL harus ditentukan untuk setiap protokol yang diaktifkan pada interface.

Satu ACL per arah - ACL mengontrol lalu lintas satu arah pada satu waktu pada satu interface. Dua ACL terpisah harus dibuat untuk mengontrol lalu lintas masuk dan keluar.

Satu ACL per interface - ACL mengontrol lalu lintas pada suatu interface, misalnya GigabitEthernet 0/0.

PENERAPAN ACL STANDART




```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

Setiap ACL diterapkan dimana akan memberikan efisiensi penulisan ataupun trafik data. Aturan baku untuk penempatan ACL bisa seperti di bawah :

Extended ACLs – Diletakkan pada sedekat mungkin dari sumber trafik (user)

Standard ACLs – Karena standart ACL tidak memberikan filter kepada alamat tujuan, maka sebisa mungkin penempatannya ada pada tujuan akhir dari trafik data (server)

PENERAPAN EXTENDED ACL

Selain bisa digunakan untuk membatasi/filter sebuah host atau range IP address ataupun sebuah network, ACL extended juga bisa digunakan untuk membuat sebuah filter berdasarkan obyek/service apa saja yang ada pada sebuah lalu lintas jaringan/atau layanan dari sebuah server.

Penulisan script bisa dengan menuliskan no port (gambar a) layanan yang dibatasi ataupun bisa menggunakan nama dari protocol (gambar b) yang dilakukan pembatasan.

Using Port Numbers

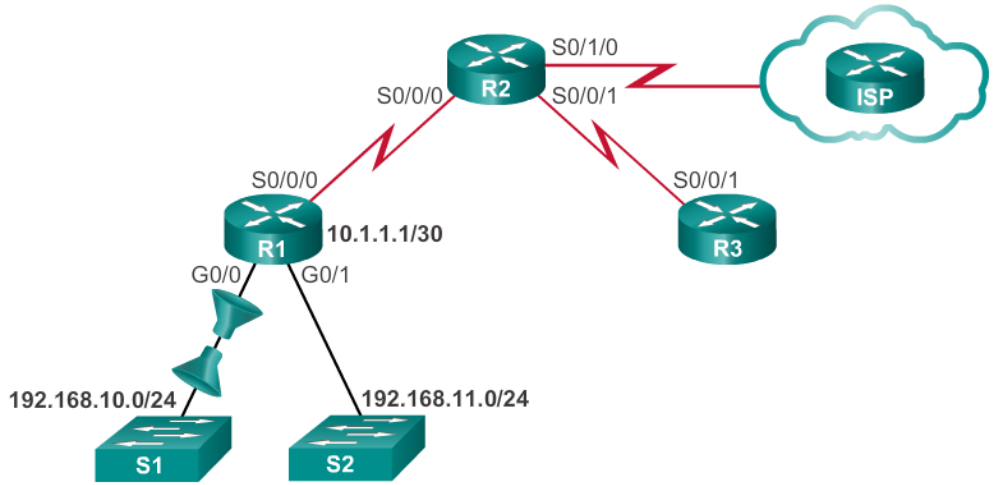
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

(a)

Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

(b)




```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

PENERAPAN ACL EXTENDED

Setiap ACL diterapkan dimana akan memberikan efisiensi penulisan ataupun trafik data. Aturan baku untuk penempatan ACL bisa seperti di bawah :

Extended ACLs – Diletakkan pada sedekat mungkin dari sumber trafik (user)

Standard ACLs – Karena standart ACL tidak memberikan filter kepada alamat tujuan, maka sebisa mungkin penempatannya ada pada tujuan akhir dari trafik data (server)

WILDCARD MASK EXAMPLES: MATCH RANGES

Range to restrict:

172.16.0.0 – 172.31.255.255

Base IP Address:

172.16.0.0

Wildcard Mask:

0.15.255.255

WILDCARD MASK EXAMPLE: MATCH RANGE

172.16.0.0

0.15.255.255

10101100 . 00010000 . 00000000 . 00000000

00000000 .00001111 . 11111111 . 11111111

Keep:

10101100 . 0001xxxx . xxxxxxxx . xxxxxxxx

Minimum:

10101100 . 00010000 . 00000000 . 00000000

Maximum:

10101100 . 00011111 . 11111111 . 11111111

WILDCARD MASK CHALLENGE:

Question: What IP addresses does this combination isolate?

Base IP Address:

192.168.20.37

Wildcard Mask:

0.0.0.254

WILDCARD MASK CHALLENGE:

192.168.20.37

0.0.0.254

11000000 . 10101000 . 00010100 . 00100101

00000000 .00000000 . 00000000 . 11111110

Keep:

11000000 . 10101000 . 00010100 . xxxxxxx1

WILDCARD MASK CHALLENGE: ANSWER!

11000000 . 10101000 . 00010100 . xxxxxxx1

Isolates all the **ODD** numbers in the

192.168.20.X

Subnet!

WILDCARD MASK KEYWORDS

Wildcard mask of:

0.0.0.0

Keeps all bits Keyword is: **Host**

255.255.255.255

Eliminates all bits Keyword is : **ANY**

EXAMPLES WILDCARD MASK KEYWORDS

Example 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

GUIDELINES FOR ACL PLACEMENT

WHERE TO PLACE ACLS

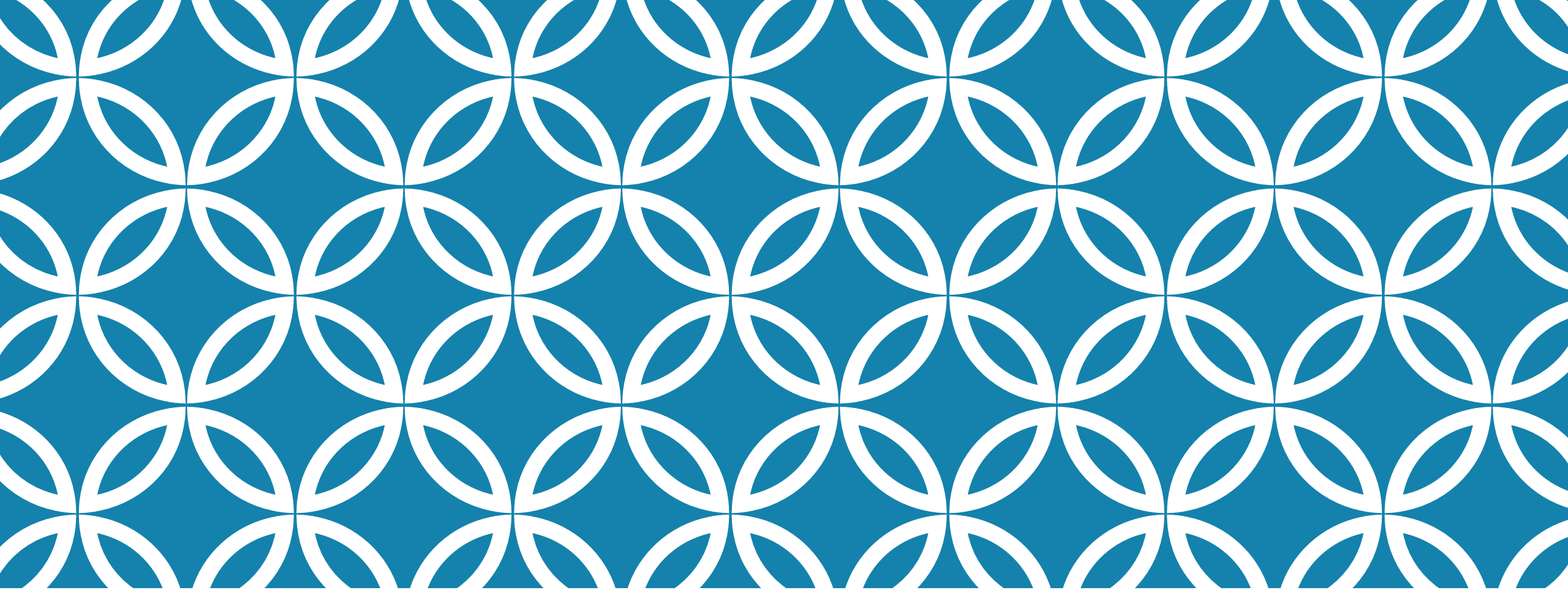
Setiap ACL harus ditempatkan di tempat yang memiliki dampak terbesar pada efisiensi. Aturan dasarnya adalah:

Extended ACLs

- Letakkan ACL sedekat mungkin dengan sumber lalu lintas yang difilter.

Standard ACLs

- Karena ACL standar tidak menentukan alamat tujuan, maka letakkan sedekat mungkin ke tujuan



TERIMA KASIH

Jaringan Komputer 2