অধ্যায়-১০

অ্যাক্সেস কন্ট্রোল লিস্ট

SOS অতি সংক্ষিপ্ত প্রশ্নোত্তর ঃ

***** ১। ACL কী?**

উত্তর ঃ ACL-এর পূর্ণরূপ হলো Access Control List. এটি মূলত একগুচ্ছ নিয়ম বা ফিল্টার, যা একটি রাউটার বা লেয়ার-৩ সুইচ ব্যবহার করে নেটওয়ার্ক ট্রাফিক নিয়ন্ত্রণ করার জন্য ব্যবহার করা হয়।

**** ২। পোর্ট সিকিউরিটি (Port Security) বলতে কী বুঝ?**

বাকাশিবো- ১৯, ২১'পরি, ২৪

উত্তর ঃ পোর্ট সিকিউরিটি হলো সিসকো সুইচের একটি গুরুত্বপূর্ণ নিরাপত্তা বৈশিষ্ট্য, যা নির্দিষ্ট কোনো পোর্টের মাধ্যমে নেটওয়ার্কে কোন ডিভাইস যুক্ত হতে পারবে তা নিয়ন্ত্রণ করে। এর মাধ্যমে নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর একটি পোর্টে কতটি এবং কোন কোন MAC Address যুক্ত হতে পারবে তা সীমাবদ্ধ করে দিতে পারেন।

SOS সংক্ষিপ্ত প্রশ্নোত্তর ঃ

***** ১। ACL এর বৈশিষ্ট্যগুলো লেখ।**

উত্তর ঃ ACL এর বৈশিষ্ট্যগুলো নিম্নরূপ ঃ

ক) প্যাকেট ফিল্টারিং ঃ ACL মূলত একটি ফিল্টার হিসেবে কাজ করে, যা নেটওয়ার্ক প্যাকেটের সোর্স আইপি, ডেস্টিনেশন আইপি এবং প্রোটোকল নম্বর যাচাই করে ট্রাফিক নিয়ন্ত্রণ করে।

খ) Permit এবং Deny স্টেটমেন্ট ঃ প্রতিটি ACL একগুচ্ছ 'Permit' (অনুমতি) এবং 'Deny' (অস্বীকৃতি) নিয়মের সমন্বয়ে গঠিত। এর মাধ্যমে নির্দিষ্ট ট্রাফিককে যেতে দেওয়া হয় অথবা ব্লক করা হয়।

গ) ক্রমিক অনুসরণ ঃ রাউটার ACL-এর নিয়মগুলো তালিকার উপর থেকে নিচে ক্রমানুসারে চেক করে। প্রথম যে নিয়মের সাথে প্যাকেটটি মিলে যায়, সেটিই কার্যকর হয়।

ঘ) ইমপ্লিসিট ডিনাই ঃ এটি ACL-এর একটি গুরুত্বপূর্ণ বৈশিষ্ট্য। যদি কোনো প্যাকেট তালিকার কোনো নিয়মের সাথেই না মিলে, তবে সেটি তালিকার শেষে থাকা অদৃশ্য একটি 'Deny' নিয়মের কারণে স্বয়ংক্রিয়ভাবে ব্লক হয়ে যায়।

ঙ) ইনবাউন্ড ও আউটবাউন্ড কন্ট্রোল ঃ ACL রাউটারের ইন্টারফেসে দুইভাবে কাজ করতে পারে– ইনবাউন্ড (প্যাকেট রাউটারে ঢোকার সময়) এবং আউটবাউন্ড (প্যাকেট রাউটার থেকে বের হওয়ার সময়)।

চ) সিকিউরিটি ও ব্যান্ডউইথ ম্যানেজমেন্ট ঃ এটি অননুমোদিত ইউজারদের আটকানোর পাশাপাশি অপ্রয়োজনীয় ট্রাফিক ব্লক করে নেটওয়ার্কের ব্যান্ডউইথ সাশ্রয় করে।

ছ) শনাক্তকরণ ঃ ACL-কে চেনার জন্য নম্বর (যেমন ঃ 1-99 বা 100-199) অথবা নাম ব্যবহার করা হয়।

**** ২। ACL এর সুবিধা ও অসুবিধা লেখ।**

উত্তর ঃ ACL ব্যবহারের সুবিধাসমূহ ঃ

ক) নিরাপত্তা বৃদ্ধি ঃ ACL ব্যবহারের প্রধান সুবিধা হলো নেটওয়ার্কের নিরাপত্তা। এটি অননুমোদিত ইউজার বা ক্ষতিকারক ট্রাফিককে নেটওয়ার্কে প্রবেশ করতে বাধা দেয়।

খ) ব্যান্ডউইথ নিয়ন্ত্রণ ঃ অপ্রয়োজনীয় ট্রাফিক বা অ্যাপ্লিকেশন (যেমন ঃ ভিডিও স্ট্রিমিং বা গেম) ব্লক করে দিয়ে গুরুত্বপূর্ণ কাজের জন্য নেটওয়ার্ক ব্যান্ডউইথ সাশ্রয় করা যায়।

গ) ট্রাফিক ফিল্টারিং ঃ এর মাধ্যমে নির্দিষ্ট পিসি বা নির্দিষ্ট নেটওয়ার্কের ওপর ভিত্তি করে ডেটা আদান-প্রদান নিয়ন্ত্রণ করা সম্ভব।

ঘ) অ্যাক্সেস লেভেল ম্যানেজমেন্ট ঃ প্রতিষ্ঠানের বিভিন্ন বিভাগের মধ্যে অ্যাক্সেস সীমাবদ্ধ করা যায়। যেমন–HR বিভাগের কেউ যেন অ্যাকাউন্টস বিভাগের সার্ভারে প্রবেশ করতে না পারে।

ঙ) সার্ভিস কন্ট্রোল (Extended ACL) ঃ এটি শুধু আইপি নয়, বরং নির্দিষ্ট সার্ভিস বা প্রোটোকল (যেমন ঃ HTTP, FTP, Telnet) ব্লক বা এলাউ করতে পারে।

ACL ব্যবহারের অসুবিধাসমূহ ঃ

ক) কনফিগারেশন জটিলতা ঃ বড় নেটওয়ার্কের জন্য অনেকগুলো রুলস বা নিয়ম তৈরি করা বেশ জটিল। একটি ছোট ভুল পুরো নেটওয়ার্কের যোগাযোগ বন্ধ করে দিতে পারে।

খ) প্রসেসিং লোড ঃ রাউটার যখন প্রতিটি প্যাকেটকে ACL-এর তালিকার সাথে মিলিয়ে দেখে, তখন রাউটারের প্রসেসরের ওপর অতিরিক্ত চাপ পড়ে। এতে নেটওয়ার্কের গতি কিছুটা কমে যেতে পারে।

গ) টপ-ডাউন এপ্রোচ ঃ ACL নিয়মগুলো উপর থেকে নিচে চেক করে। তাই নিয়মের ক্রম বা সিরিয়াল ভুল হলে কাঙ্ক্ষিত ফলাফল পাওয়া যায় না।

ঘ) ইমপ্লিসিট ডিনাই (Implicit Deny) ঃ ACL-এর শেষে একটি অদৃশ্য 'Deny Any' রুল থাকে। যদি অ্যাডমিনিস্ট্রেটর শেষে 'Permit Any' দিতে ভুলে যান, তবে বৈধ ট্রাফিকও ব্লক হয়ে যেতে পারে।

ঙ) সফটওয়্যার সীমাবদ্ধতা ঃ সাধারণ ACL অ্যাপ্লিকেশন লেয়ারের ভাইরাস বা ম্যালওয়্যার শনাক্ত করতে পারে না। এটি কেবল আইপি এবং পোর্টের ওপর ভিত্তি করে কাজ করে।

**** ৩। ACL এর কাজ লেখ।**

উত্তর ঃ ACL (Access Control List)-এর প্রধান কাজগুলো নিম্নরূপ ঃ

ক) ট্রাফিক ফিল্টারিং ঃ নেটওয়ার্কের ভেতর দিয়ে আসা-যাওয়া করা ডাটা প্যাকেটগুলো পরীক্ষা করা এবং নির্দিষ্ট নিয়ম অনুযায়ী সেগুলো অনুমতি দেওয়া (Permit) বা ব্লক (Deny) করা।

খ) নিরাপত্তা প্রদান ঃ অননুমোদিত ইউজার বা হ্যাকারদের নেটওয়ার্কের গুরুত্বপূর্ণ সার্ভার বা ডিভাইসে প্রবেশ করতে বাধা দিয়ে নিরাপত্তা নিশ্চিত করা।

গ) সার্ভিস নিয়ন্ত্রণ ঃ নির্দিষ্ট প্রোটোকল বা সার্ভিস (যেমন ঃ HTTP, FTP, Telnet) নিয়ন্ত্রণ করা। অর্থাৎ, কে ইন্টারনেট চালাতে পারবে বা কে ফাইল শেয়ার করতে পারবে তা নির্ধারণ করা।

ঘ) ব্যান্ডউইথ সাশ্রয় ঃ অপ্রয়োজনীয় ট্রাফিক বা বিনোদনমূলক সাইটের ডাটা ব্লক করে দিয়ে কাজের জন্য পর্যাপ্ত ইন্টারনেট গতি বজায় রাখা।

ঙ) রিমোট অ্যাক্সেস সিকিউরিটি ঃ রাউটার বা সুইচে দূর থেকে (Telnet/SSH) কারা লগইন করতে পারবে তা সীমাবদ্ধ করে দেওয়া।

চ) মনিটরিং ঃ নেটওয়ার্কে কোন ধরণের ডাটা বেশি যাতায়াত করছে বা কারা ঢোকার চেষ্টা করছে তার লগ রাখা।